

1 Sean P. Killeen (SBN 320644)  
2 *skilleen@bakerlaw.com*  
3 **BAKER & HOSTETLER LLP**  
4 Transamerica Pyramid Center  
5 600 Montgomery Street, Suite 3100  
6 San Francisco, CA 94111  
7 Telephone: 415.659.2600  
8 Facsimile: 415.659.2601

9 Casie D. Collignon (*Pro Hac Vice* Application  
10 Forthcoming)  
11 *ccollignon@bakerlaw.com*  
12 Jonathan Maddalone (*Pro Hac Vice* Application  
13 Forthcoming)  
14 *jmaddalone@bakerlaw.com*

15 **BAKER & HOSTETLER LLP**  
16 1801 California Street, Suite 4400  
17 Denver, CO 80202-2662  
18 Telephone: 303.861.0600  
19 Facsimile: 303.861.7805

20 Attorneys for Defendant  
21 BANNER HEALTH

22 **UNITED STATES DISTRICT COURT**  
23 **EASTERN DISTRICT OF CALIFORNIA**

24 JOHN DOE, individually, and on behalf  
25 of all others similarly situated,

26 Plaintiff,

27 v.

28 BANNER HEALTH,

Defendant.

Case No.:

**NOTICE OF REMOVAL OF  
ACTION UNDER 28 U.S.C.  
§§ 1332, 1446 AND 1453  
(DIVERSITY JURISDICTION  
UNDER CLASS ACTION  
FAIRNESS ACT)**

Date Action Filed: March 14, 2024  
Complaint Served: March 20, 2024

**TO THE CLERK OF THE ABOVE-ENTITLED COURT:**

**PLEASE TAKE NOTICE** that defendant Banner Health (“Defendant” or “Banner”) removes the above-captioned action, pending in the Superior Court of California, County of Lassen, Case No. 2024CV76564 (the “State Court Action”) to the United States District Court, Eastern District of California, pursuant to the Class Action Fairness Act (“CAFA”) of 2005, codified in part at 28 U.S.C. § 1332(d). In support, Banner provides the following “short and plain statement of the grounds for removal.” 28 U.S.C. § 1446(a); *see also Dart Cherokee Basin Operating Co., LLC v. Owens*, 574 U.S. 81, 87 (2014) (“*Dart Cherokee*”).

**I. NATURE OF THE CASE**

1. This is one of numerous website privacy cases that have been filed against health care providers and systems across the country that involve nearly identical facts and claims.

2. On March 14, 2024, plaintiff John Doe (“Plaintiff”), individually and on behalf of all others similarly situated, filed the Class Action Complaint for Damages (the “Complaint” or “Compl.”) in this civil action against defendant Banner Health, in the Superior Court of California, County of Lassen, Case No. 2024-cv-0076564. [See Exhibit 1, Compl.] True and correct copies of all other documents filed in state court, along with the state court docket sheet are attached as Exhibit 2.

3. Plaintiff alleges that Banner violated California law by embedding certain third-party source code—called the Meta Pixel—onto Banner’s publicly available websites referred to in the Complaint as the “Website” and “Online Platforms.” [Compl., at ¶¶ 8-11, 16-18.]

4. In addition to the Meta Pixel, Plaintiff alleges that Banner violated California and federal law by installing other tracking technologies which Plaintiff claims operate similarly to the Meta Pixel and transmit a website user’s Private Information to other third parties. [*Id.* at ¶ 19.]

1           5. Plaintiff alleges that these tracking tools, including the Meta Pixel, are  
 2 “piece[s] of code” that collect data on users as they navigate Banner’s Website and  
 3 Online Platforms, including content viewed, buttons clicked by site visitors,  
 4 appointment activities, patient forms, and insurance information. [*Id.* at ¶¶ 6-7, 54,  
 5 57, 99.]

6           6. Plaintiff alleges that Banner “willfully and intentionally incorporat[ed]  
 7 the Meta Pixel, potentially CAPI, and other third-party trackers into their Websites  
 8 and Servers[.]” [*Id.* at ¶ 22.] As a result, Banner “surreptitiously forc[ed] Plaintiff  
 9 and Class Members to transmit intimate details about their medical treatment to  
 10 third parties without their consent.” [*Id.* at ¶ 8.]

11           7. Plaintiff alleges that he has been a patient of Banner since 2008 and  
 12 that he has been accessing the Website and Online Platforms since 2021 to search  
 13 and communicate “confidential patient information,” including, among other  
 14 activities, using the Website’s search function to search for health information on  
 15 spinal degeneration, and searching for physicians. [*Id.* at ¶¶ 149-51.] Notably,  
 16 Plaintiff’s allegations do not focus on his individual patient status but rather they  
 17 focus on his mere usage of Banner’s public website. [*Id.*]

18           8. Plaintiff alleges ten causes of action against Banner under California  
 19 and federal law: (1) negligence [*id.* at ¶¶ 224-40]; (2) breach of implied contract [*id.*  
 20 at ¶¶ 241-51]; (3) unjust enrichment [*id.* at ¶¶ 252-59]; (4) breach of fiduciary duty  
 21 [*id.* at ¶¶ 260-66]; (5) invasion of privacy – intrusion upon seclusion [*id.* at ¶¶ 267-  
 22 76]; (6) invasion of privacy under the California Constitution, Cal. Const. Art. 1 § 1  
 23 [*id.* at ¶¶ 277-87]; (7) an alleged violation of the California Invasion of Privacy Act  
 24 (“CIPA”), Cal. Penal Code §§ 630, *et seq.* [*id.* at ¶¶ 288-307]; (8) Violation of the  
 25 California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.06,  
 26 56.10, 56.101 [*id.* at ¶¶ 308-24]; (9) Violation of the Comprehensive Computer  
 27 Data Access and Fraud Act (“CDAFA”), Cal. Penal Code § 502 [*id.* at ¶¶ 325-37];  
 28 and (10) Violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.* [*id.* at ¶¶ 338-61].

1 Plaintiff asserts these claims on behalf of a nationwide class. [*Id.* at ¶ 209.]

## 2 **II. NO ADMISSION**

3 9. Banner denies any liability in this case, both as to Plaintiff's individual  
4 claims and as to the claims of the members of the putative class. In alleging the  
5 amount in controversy and other matters in this removal pleading, Banner does not  
6 concede any liability, damages, or any other claims or defenses. Banner is only  
7 stating what the stakes of litigation could be under Plaintiff's allegations as set forth  
8 in his Complaint.

## 9 **III. VENUE IS PROPER IN THIS COURT**

10 10. Venue is proper in this Court because this Court is within a judicial  
11 district and division embracing the place where the state court case was brought and  
12 is pending. The civil action was filed with the Superior Court of California, County  
13 of Lassen, a court within the Eastern District of California. Thus, this Court is a  
14 proper district court to which this case should be removed. *See* 28 U.S.C. §§  
15 1441(a), 1446(a). However, this is not the most appropriate venue for this action as  
16 virtually identical allegations in other previously filed actions, which have since  
17 been consolidated, are pending in the District of Arizona, *McCulley et al. v. Banner*  
18 *Health*, Case No. 2:23-CV-0985-SPL. In the interests of transparency, seven (7) of  
19 Plaintiff's causes of action are already alleged on behalf of a nationwide class and  
20 California subclass. *Id.* at Dkt. 23 ¶¶ 278, 280. Accordingly, upon removal, Banner  
21 intends to file a motion to transfer venue to conserve resources and ensure  
22 consistency in the litigation.

## 23 **IV. JURISDICTION IS PROPER IN THIS COURT**

24 11. This is a civil action over which the Court has original subject matter  
25 jurisdiction under 28 U.S.C. § 1332, and removal is proper under the Class Action  
26 Fairness Act of 2005 ("CAFA"), codified in pertinent part at 28 U.S.C. § 1332(d).

27 12. Section 1332(d) provides that a district court shall have original  
28 jurisdiction over a class action with one hundred or more putative class members, in



1 which the aggregate amount in controversy exceeds \$5 million. Section 1332(d)  
 2 further provides that, for original jurisdiction to exist, “any member of a class of  
 3 plaintiffs” must be a “citizen of a State different from any Defendant.” *See* 28  
 4 U.S.C. § 1332(d)(2)(A).

5 13. There is no presumption against removal under CAFA. *See, e.g., Dart*  
 6 *Cherokee*, 574 U.S. at 89 (“[N]o antiremoval presumption attends cases invoking  
 7 CAFA, which Congress enacted to facilitate adjudication of certain class actions in  
 8 federal court.”). To the contrary, “CAFA’s ‘provisions should be read broadly,  
 9 with a strong preference that interstate class actions should be heard in federal court  
 10 if properly removed by any defendant.’” *Id.* at 554 (quoting S. Rep. No. 109-14, p.  
 11 43 (2005)).

12 14. As demonstrated below, pursuant to 28 U.S.C. § 1332(d) and §  
 13 1441(a), Banner may remove this action to this federal court under CAFA because:  
 14 (1) this action is pled as a class action; (2) the putative class includes more than one  
 15 hundred members; (3) minimal diversity exists; and (4) the aggregate matter in  
 16 controversy exceeds the sum or value of \$5,000,000.00, exclusive of interest and  
 17 costs.

18 15. As set forth below, because all CAFA requirements are satisfied here,  
 19 removal of this action is appropriate.

## 20 **V. THIS ACTION IS PLED AS A CLASS ACTION**

21 16. As a threshold matter, this civil action qualifies as a putative class  
 22 action because Plaintiff seeks to certify a class of “hundreds or thousands” of  
 23 individuals whose information may have been “improperly used or disclosed” by  
 24 Banner. [*See* Compl., ¶ 212.]

25 17. Plaintiff brings the Complaint “as a class action” under California  
 26 Code of Civil Procedure § 382 and seeks certification of a putative nationwide  
 27 class. [*Id.* at ¶ 209.] Thus, the first CAFA requirement is satisfied.  
 28

1 **VI. THE PUTATIVE CLASS INCLUDES AT LEAST ONE HUNDRED**  
 2 **MEMBERS**

3 18. Plaintiff alleges in the Complaint that, “[u]pon information and belief,  
 4 there are hundreds or thousands of individuals whose Private Information may have  
 5 been “improperly used or disclosed” by Banner, and the class is “identifiable within  
 6 [Banner]’s records.” [Compl., ¶ 212.] Therefore, the putative class includes at  
 7 least one hundred members, and the numerosity requirement is satisfied under  
 8 CAFA.

9 **VII. THERE IS SUFFICIENT DIVERSITY OF CITIZENSHIP**

10 19. Pursuant to 28 U.S.C. § 1332(d)(2)(A), the “district court shall have  
 11 original jurisdiction” over a “class in which . . . *any member of the class of*  
 12 *plaintiffs* is a citizen of a State different from *any defendant*.” (emphasis added).  
 13 *See also Abrego v. Dow Chem. Co.*, 443 F.3d 676, 680 n.5 (9th Cir. 2006) (“One  
 14 way to satisfy minimal diversity is by demonstrating that any member of a class of  
 15 plaintiffs is . . . a citizen or subject of a foreign state and any defendant is a citizen  
 16 of a State.”) (internal citations omitted).

17 20. Plaintiff is a Citizen of California. Plaintiff alleges in the Complaint  
 18 that he is a resident of California. [Compl., ¶ 29.] For diversity purposes, a person  
 19 is a “citizen” of the state in which he or she is domiciled. *Kantor v. Wellesley*  
 20 *Galleries, Ltd.*, 704 F.2d 1088, 1090 (9th Cir. 1983). Residence is *prima facie*  
 21 evidence of domicile. *State Farm Mut. Auto Ins. Co. v. Dyer*, 19 F.3d 514, 520  
 22 (10th Cir. 1994). At this stage of the litigation, Banner has met its burden to show  
 23 that Plaintiff is a citizen of the State of California.

24 21. Banner is a Citizen of Arizona. Pursuant to 28 U.S.C. § 1332(c), “a  
 25 corporation shall be deemed to be a citizen of every State . . . by which it has been  
 26 incorporated and of the State . . . where it has its principal place of business.” The  
 27 United States Supreme Court has concluded that a corporation’s “principal place of  
 28 business” is “where a corporation’s officers direct, control, and coordinate the

corporation's activities," or its "nerve center." *Hertz Corp. v. Friend*, 130 S. Ct. 1181, 1192 (2010). "[I]n practice," a corporation's "nerve center" should "normally be the place where the corporation maintains its headquarters." *Id.* "The public often (though not always) considers it the corporation's main place of business." *Id.* at 1193. Plaintiff alleges that Banner is a not-for-profit corporation organized and existing under the laws of the State of Arizona with its principal place of business at 2901 North Central Avenue, Suite 160, Phoenix, Arizona 85012 in Maricopa County. [Compl., ¶ 30.] As Banner is a citizen of Arizona for purposes of evaluating diversity, minimal diversity of citizenship is established pursuant to CAFA.

# **VIII. THE AMOUNT IN CONTROVERSY EXCEEDS THE CAFA THRESHOLD**

22. The Amount in Controversy Exceeds the CAFA Threshold. Where, as here, a complaint does not specify the amount of damages sought, the removing defendant must prove by a preponderance of the evidence that the jurisdictional amount-in-controversy is satisfied. 28 U.S.C. § 1446(c)(2)(B). It is well established that "a defendant's notice of removal need include only a plausible allegation that the amount in controversy exceeds the jurisdictional threshold" to meet the amount in controversy requirement. *See e.g., Dart Cherokee*, 574 U.S. at 89. The burden of establishing the jurisdictional threshold "is not daunting, as courts recognize that under this standard, a removing defendant is not obligated to research, state, and prove the plaintiff's claims for damages." *Korn v. Polo Ralph Lauren Corp.*, 536 F. Supp. 2d 1199, 1204-05 (E.D. Cal. 2008) (internal quotations omitted).

23. The claims of the individual class members in a "class action" are aggregated to determine if the amount in controversy exceeds the sum or value of \$5,000,000.00. *See* 28 U.S.C. §§ 1332(d)(6), (11). Congress intended for federal jurisdiction to be appropriate under CAFA "if the value of the matter in litigation exceeds \$5,000,000.00 either from the viewpoint of the plaintiff or the viewpoint of

1 the defendant, and regardless of the type of relief sought (*e.g.*, damages, injunctive  
2 relief, or declaratory relief).” Senate Judiciary Committee Report, S. Rep. 109-14,  
3 at 42. Moreover, the Senate Judiciary Committee’s Report on the final version of  
4 CAFA makes clear that any doubts regarding the maintenance of interstate class  
5 actions in state or federal court should be resolved in favor of federal jurisdiction.

6 24. The Ninth Circuit has also found that any doubts over the amount in  
7 controversy in a CAFA action should be resolved in favor of federal jurisdiction.  
8 *See, e.g., Benko v. Quality Loan Serv. Corp.*, 789 F.3d 1111, 1116 (9th Cir. 2015)  
9 (““CAFA’s language favors federal jurisdiction over class actions.””) (quoting  
10 *Evans v. Walter Indus., Inc.*, 449 F.3d 1159, 1163 (11th Cir. 2006) (“CAFA’s  
11 language favors federal jurisdiction over class actions and CAFA’s legislative  
12 history suggests that Congress intended ... all doubts [be] resolved ‘in favor of  
13 exercising jurisdiction over the case.’”)); *Jordan v. Nationstar Mortg. LLC*, 781  
14 F.3d 1178, 1181 (9th Cir. 2015) (“Congress and the Supreme Court have instructed  
15 us to interpret CAFA’s provisions under section 1332 broadly in favor of removal,  
16 and we extend that liberal construction to section 1446.”).

17 25. As demonstrated below, the allegations in the Complaint plausibly  
18 establish that the amount in controversy at issue exceeds \$5,000,000.00.

19 26. Plaintiff’s Alleged Damages. Plaintiff alleges he has suffered injuries,  
20 including monetary damages, loss of privacy, unauthorized disclosure of his Private  
21 Information, unauthorized access to his Private Information by third parties, use of  
22 the Private Information for advertising purposes, embarrassment, humiliation,  
23 frustration, and emotional distress, decreased value of his Private Information, lost  
24 benefit of the bargain, and increased risk of future harm resulting from further  
25 unauthorized use and disclosure. [Compl., ¶¶ 158.] As a result, Plaintiff seeks an  
26 award of actual damages, compensatory damages, statutory damages, statutory  
27 penalties, and for an award of punitive damages. [*Id.* at ¶¶ 236-40, 250-51, 257,  
28 266, 274-75, 284-86, 305-06, 322-23, 336, Prayer for Relief.] Plaintiff further

1 seeks injunctive relief and attorneys' fees. [*Id.* at ¶¶ 222-23, 266, 305, 322, 336,  
2 361, Prayer for Relief.]

3 27. Plaintiff's claims for statutory damages alone far exceeds the  
4 \$5,000,000.00 minimal threshold under CAFA.

5 28. Claim for an Alleged Violation of the California Invasion of Privacy  
6 Act ("CIPA"). Plaintiff alleges that Banner violated CIPA and that because of  
7 Banner's purported conduct, Plaintiff and the putative class members are entitled, in  
8 part, to statutory damages under Cal. Penal Code § 637.2. [Compl., ¶¶ 288-307.]  
9 Cal. Penal Code § 637.2 provides for the greater of: (1) \$5,000.00 per violation; or  
10 (2) three times the amount of damages sustained by Plaintiff and the Class in an  
11 amount to be proven at trial, as well as injunctive or other equitable relief. [*Id.* at ¶  
12 305.]

13 29. Here, Plaintiff alleges that Banner is a "massive, national health care  
14 system" that "provides treatment to services to patients in Arizona, California,  
15 Colorado, Nebraska, Nevada, Wyoming, and in Alaska through 28 hospitals and a  
16 growing network of health centers and clinics." [*Id.* at ¶ 35.] Plaintiff's proposed  
17 nationwide class is not limited only to patients of Banner. Instead, Plaintiff's  
18 proposed nationwide class includes "[a]ll *persons* whose Private Information was  
19 disclosed by Defendant to third parties through the Meta Pixel and related  
20 technology without authorization." [*Id.* at ¶ 209] (emphasis added). As evidenced  
21 by the allegations in the Complaint and the proposed class definition, Plaintiff's  
22 proposed class includes every single individual who may have used Banner's public  
23 website in some capacity. [*Id.* at ¶¶ 75-78, 150-51, 209.]

24 30. When analyzing Plaintiff's allegations, the statutory damages from  
25 CIPA alone meet the amount in controversy threshold. CIPA establishes, at  
26 minimum, statutory damages of at \$5,000.00 per violation. [Cal. Penal Code §  
27 637.2; Compl., ¶ 305.] Operating 28 hospitals and various health centers and  
28 clinics across several states, it is plausible that Banner's public website was visited

1 over 1,000 times. [*Id.* at ¶ 35.] For example, over the course of a year, only 84  
 2 California citizens would have had to visit Banner’s public website per month for  
 3 California citizens alone to qualify for statutory damages that exceed  
 4 \$5,000,000.00. Therefore, the statutory damages for CIPA easily establishes the  
 5 amount in controversy requirement.

6 31. Claim for an Alleged Violation of the California Confidentiality of  
 7 Medical Information Act (“CMIA”). Plaintiff also alleges that Banner violated the  
 8 CMIA “by failing to maintain the confidentiality of users’ medical information,  
 9 Private Information, and instead, disclosing Plaintiff’s and Class Members’ medical  
 10 information/Private Information to Facebook and likely other third parties without  
 11 consent.” [Compl., ¶ 311.] Under Cal. Civil Code § 56.36(b)(1), Plaintiff alleges  
 12 that he and the putative class members are entitled to nominal damages of  
 13 \$1,000.00 per violation for Banner’s failure to “maintain, preserve, and store  
 14 medical information” consistent with CMIA, and that Banner is liable for civil  
 15 penalties pursuant to Cal. Civil Code § 56.36(c), which can range from \$2,500.00 to  
 16 \$25,000.00 per violation of CMIA. [*Id.* at ¶ 321-22.]

17 32. Similar to the statutory damages under CIPA, the amount in  
 18 controversy is met based on CMIA statutory damages alone. Under the CMIA,  
 19 Banner could be liable for at least \$1,000.00 per violation, [*Id.* at ¶ 322.] and could  
 20 be liable for additional civil penalties that range from \$2,500.00 to \$25,000.00 per  
 21 violation of CMIA. Cal. Civil Code § 56.36(c). Given Plaintiff’s allegations  
 22 concern the mere visitation of Banner’s public website, a mere 5,000 California  
 23 citizens would have to visit Banner’s public website, or 139 individuals per month  
 24 over the course of three years, for the CMIA’s nominal damages alone to qualify.  
 25 Notwithstanding the additional civil penalties, it is clear that Plaintiff’s claim under  
 26 CMIA, by itself, seeks damages exceeding the \$5,000,000.00 jurisdictional  
 27 threshold.  
 28



33. Attorneys' Fees: When the underlying substantive law provides for the award of attorneys' fees, a party may include that amount in their calculation of the amount in controversy. *Galt G/S v. JSS Scandinavia*, 142 F.3d 1150, 1156 (9th Cir. 1998). The Court may consider reasonable estimates of attorneys' fees when analyzing disputes over the amount in controversy. *See Brady v. Mercedes-Benz USA, Inc.*, 243 F. Supp. 2d 1004, 1010-11 (N.D. Cal. 2002). Plaintiff seeks attorneys' fees here. [Compl. ¶¶ 322, 336, 361, Prayer for Relief.] Attorneys' fees should therefore be included in analyzing the amount in controversy. In the Ninth Circuit, 25% of the award has been used as a "benchmark" for attorneys' fees. *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1029 (9th Cir. 1998). Using this benchmark, attorneys' fees, when added to the amounts discussed above, further increase the amount in controversy for alleged liability exposure above the jurisdictional minimum for removal.

34. Other Damages: In addition to the damages discussed above, Plaintiff also seeks punitive damages and injunctive relief (among other forms of relief not calculated above) on behalf of himself and all putative class members. [Compl., ¶¶ 222-23, 266, 239-40, 275, 286, 305, 336, 361, Prayer for Relief]; *See also Gibson v. Chrysler Corp.*, 261 F.3d 927, 946 (9th Cir. 2001), holding modified by *Exxon Mobil Corp. v. Allapattah Services, Inc.*, 545 U.S. 546 (2005) (finding that the potential for punitive damages may still be considered for purposes of amount in controversy); *see also Hunt v. Wash. State Apple Adver. Comm'n*, 432 U.S. 333, 347 (1977) ("In actions seeking . . . injunctive relief, it is well established that the amount in controversy is measured by the value of the object of the litigation."). No allegations in the Complaint allow Banner to calculate the amount of these alleged damages and relief. However, these additional damages, combined with the statutory damages and requests for attorneys' fees plausibly establish that the amount in controversy exceeds \$5,000,000.00.



1 **IX. PROCEDURAL REQUIREMENTS FOR REMOVAL**

2 35. Banner satisfies all the procedural requirements under 28 U.S.C. §  
3 1332(d).

4 36. Plaintiff served Banner with a partial Complaint on March 20, 2024,  
5 and Banner filed this notice of removal within thirty days of its receipt of the  
6 Complaint pursuant to 28 U.S.C. § 1446; *Murphy Bros., Inc. v. Michetti Pipe*  
7 *Stringing, Inc.*, 526 U.S. 344, 354-56 (1999).

8 37. As required by 28 U.S.C. § 1446(d), Banner is providing written notice  
9 of the filing of this Notice of Removal to Plaintiff and is filing a copy of this Notice  
10 of Removal with the Clerk of the Superior Court of the State of California, County  
11 of Lassen.

12 WHEREFORE, Defendant Banner Health removes this action from the  
13 Superior Court of the State of California, County of Lassen, to the United States  
14 District Court for the Eastern District of California.

15  
16 Dated: April 19, 2024

Respectfully submitted,

17 **BAKER & HOSTETLER LLP**

18  
19 By: /s/ Sean P. Killeen  
20 Sean P. Killeen

21 Attorney for Defendant  
22 Banner Health  
23  
24  
25  
26  
27  
28

# **EXHIBIT 1**

MAR 14 2024

DEPUTY CLERK

C. Crosby

Andrew Gunem (354042)  
TURKE & STRAUSS, LLP  
613 Williamson Street, Suite 201  
Madison, Wisconsin 53703  
(608) 237-1775  
andrewg@turkestrauss.com

Lynn A. Toops\*  
Mary Kate Dugan\*  
COHEN & MALAD, LLP  
One Indiana Square, Suite 1400  
Indianapolis, Indiana 46204  
(317) 636-6481  
[ltoops@cohenandmalad.com](mailto:ltoops@cohenandmalad.com)  
[mdugan@cohenandmalad.com](mailto:mdugan@cohenandmalad.com)

Natalie A. Lyons (293026)  
Vess A. Miller (278020)  
COHEN & MALAD, LLP  
One Indiana Square, Suite 1400  
Indianapolis, Indiana 46204  
(317) 636-6481  
[nlyons@cohenandmalad.com](mailto:nlyons@cohenandmalad.com)  
[vmiller@cohenandmalad.com](mailto:vmiller@cohenandmalad.com)

J. Gerard Stranch, IV\*  
Andrew E. Mize\*  
STRANCH, JENNINGS & GARVEY, PLLC  
223 Rosa L. Parks Avenue, Suite 200  
Nashville, Tennessee 37203  
(615) 254-8801  
[gstranch@stranchlaw.com](mailto:gstranch@stranchlaw.com)  
[amize@stranchlaw.com](mailto:amize@stranchlaw.com)

*Counsel for Plaintiff and the Proposed Class*

\*To move for *pro hac vice* admission

**SUPERIOR COURT FOR THE STATE OF CALIFORNIA  
FOR THE COUNTY OF LASSEN**

2024 CV 0 07 6 5 6 4

JOHN DOE, individually and on behalf of  
all others similarly situated,

Case No. \_\_\_\_\_

Plaintiff,

**CLASS ACTION COMPLAINT  
FOR DAMAGES AND INJUNCTIVE  
RELIEF BASED UPON:**

v.

BANNER HEALTH

Defendant.

- (1) Negligence;
- (2) Breach of Implied Contract;
- (3) Unjust Enrichment;
- (4) Breach of Fiduciary Duty;
- (5) Invasion of Privacy;
- (6) Invasion of Privacy under the California Constitution, Cal. Const. Art. I § 1;
- (7) Violation of the California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq.*
- (8) Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56.06, 56.10, 56.101;
- (9) Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and,
- (10) Violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*

**JURY TRIAL DEMANDED**

**FILE  
BY FAX**

## CLASS ACTION COMPLAINT

Plaintiff, JOHN DOE, Individually, and on behalf of all others similarly situated (hereinafter, "Plaintiff"), brings this Class Action Complaint against Defendant, BANNER HEALTH (hereinafter, "Banner" or "Defendant"), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows.

### INTRODUCTION

1. Plaintiff brings this class action to address Defendant's improper practice of disclosing the confidential Personally Identifying Information ("PII")<sup>1</sup> and/or Protected Health Information ("PHI")<sup>2</sup> (collectively referred to as "Private Information") of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta ("Facebook" or "Meta"),<sup>3</sup> Google, LLC ("Google"), Microsoft, AppDynamics, Taboola, Pinterest, StackAdapt,

---

<sup>1</sup> The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

<sup>2</sup> Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last accessed Apr. 16, 2020). Banner is clearly a "covered entity" and some of the data compromised in the Disclosure that this action arises out of is "protected health information," subject to HIPAA.

<sup>3</sup> Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiff's reference to both "Facebook" and "Meta" throughout this complaint refer to the same company.

1 LinkedIn, Skai, Medallia, and potentially others via tracking technologies used on its website (“the  
2 Disclosure”).

3       2.       The Office for Civil Rights (“OCR”) at the U.S. Department of Health and Human  
4 Services (“HHS”) and the Federal Trade Commission (“FTC”) warn about the “serious privacy  
5 and security risks related to the use of online tracking technologies” present on websites or online  
6 platforms, such as Defendant’s, that “impermissibly disclos[e] consumers’ sensitive personal  
7 health information to third parties.”<sup>4</sup> OCR and FTC agree that such tracking technologies, like  
8 those present on Defendant’s website, “can track a user’s online activities” and “gather identifiable  
9 information about users as they interact with a website or mobile app, often in ways which are not  
10 avoidable by and largely unknown to users.”<sup>5</sup> OCR and FTC warn that “[i]mpermissible  
11 disclosures of an individual’s personal health information to third parties may result in a wide  
12 range of harms to an individual or others. Such disclosures can reveal sensitive information  
13 including health conditions, diagnoses, medications, medical treatments, frequency of visits to  
14 health care professionals, where an individual seeks medical treatment, and more. In addition,  
15 impermissible disclosures of personal health information may result in identity theft, financial loss,  
16 discrimination, stigma, mental anguish, or other serious negative consequences to the reputation,  
17 health, or physical safety of the individual or to others.”<sup>6</sup>

18       3.       Information about a person’s physical and mental health is among the most  
19 confidential and sensitive information in our society, and the mishandling of medical information  
20 can have serious consequences, including discrimination in the workplace or denial of insurance  
21

---

22 <sup>4</sup> Re: Use of Online Tracking Technologies, U.S. Dep’t of Health & Human Services (July 20,  
23 2023), available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), attached as Exhibit A.

<sup>5</sup> *Id.*

<sup>6</sup> Re: Use of Online Tracking Technologies, Exhibit A.

1 coverage. If people do not trust that their medical information will be kept private, they may be  
2 less likely to seek medical treatment, which can lead to more serious health problems down the  
3 road. In addition, protecting medical information and making sure it is kept confidential and not  
4 disclosed to anyone other than the person's medical provider is necessary to maintain public trust  
5 in the healthcare system as a whole.

6 4. Recognizing these facts, and in order to implement requirements of the Health  
7 Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards  
8 for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule")  
9 governing how health care providers must safeguard and protect Private Information. Under the  
10 HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable  
11 protected health information to a third party without express written authorization.

12 5. Headquartered in Phoenix, Arizona, Banner is a massive, national health care  
13 system treating patients in six (6) western states under a mission of "*making health care easier,*  
14 *so life can be better.*"<sup>7</sup>

15 6. Despite its unique position as a massive and trusted healthcare provider, Banner  
16 knowingly configured and implemented into its website, <https://www.bannerhealth.com/> (the  
17 "Website") code-based tracking devices known as "pixels" (also referred to as "trackers" or  
18 "tracking technologies"), which collected and transmitted patients' Private Information to  
19 Facebook and other third parties, without patients' knowledge or authorization.

20 7. Defendant encourages patients to use its Website, along with its various web-based  
21 tools and services (collectively, the "Online Platforms"), to learn about Banner on its main  
22  
23

---

<sup>7</sup> <https://www.bannerhealth.com/about> (last accessed March 8, 2024) (emphasis in original)

homepage,<sup>8</sup> to search for health information,<sup>9</sup> to find a doctor,<sup>10</sup> to find locations,<sup>11</sup> to learn about medical conditions and treatment services,<sup>12</sup> to learn about classes and events,<sup>13</sup> to access a patient portal,<sup>14</sup> to pay bills,<sup>15</sup> and more.

8. When Plaintiff and Class Members used Defendant's Website and Online Platforms, they thought they were communicating exclusively with their trusted healthcare provider. Unbeknownst to them, Defendant embedded pixels from Facebook, Google, and likely others, into its Website and Online Platforms, surreptitiously forcing Plaintiff and Class Members to transmit intimate details about their medical treatment to third parties without their consent.

9. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of code embedded into a website that tracks information about its visitors and their website interactions.<sup>16</sup> When a person visits a website with an embedded pixel, the pixel tracks "events" (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information submitted.<sup>17</sup> Then, the pixel transmits the event information back to the website server and to third parties, where it can be combined with other data and used for marketing.<sup>18</sup>

<sup>8</sup> <https://www.bannerhealth.com/> (last acc. Mar. 8, 2024).

<sup>9</sup> E.g., search for "chest pain," avail. at <https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

<sup>10</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

<sup>11</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

<sup>12</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

<sup>13</sup> <https://www.bannerhealth.com/calendar> (last acc. Mar. 8, 2024).

<sup>14</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).

<sup>15</sup> <https://bannerhealth.simplepay.com/app/login> (last acc. Mar. 8, 2024).

<sup>16</sup> See Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/> (last accessed Mar. 19, 2023).

<sup>17</sup> See Conversion Tracking, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking> (last visited May 22, 2023).

<sup>18</sup> *Id.*



1           10. Among the trackers Defendant embedded into its Website is the Facebook Pixel  
 2 (also referred to as the “Meta Pixel” or “Pixel”). By default, the Meta Pixel tracks information  
 3 about a visitor’s device, including their IP address, and the pages viewed.<sup>19</sup> When configured to  
 4 do so, the Meta Pixel can track much more, including a visitor’s search terms, button clicks, and  
 5 form submissions.<sup>20</sup> Additionally, the Meta Pixel can link a visitor’s website interactions with an  
 6 individual’s unique and persistent Facebook ID (“FID”), allowing a user’s health information to  
 7 be linked with their Facebook profile.<sup>21</sup>

8           11. Operating as designed and as implemented by Defendant, the Meta Pixel allowed  
 9 Defendant to unlawfully disclose Plaintiff and Class Members’ Private Health Information  
 10 alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant  
 11 effectively planted a bug on Plaintiff’s and Class Members’ web browsers and compelled them to  
 12 disclose Private Information and confidential communications to Facebook without their  
 13 authorization or knowledge.

14           12. Facebook encourages and recommends use of its Conversions Application  
 15 Programming Interface (“CAPI”) alongside use of the Meta Pixel.<sup>22</sup>

---

17 <sup>19</sup> See Get Started, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/get-started> (last visited May 22, 2023).

18 <sup>20</sup> See Conversion Tracking, META FOR DEVELOPERS,  
 19 <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking> (last  
 visited May 22, 2023).

20 <sup>21</sup> The Meta Pixel forces the website user to share the user’s FID for easy tracking via the “cookie”  
 Facebook stores every time someone accesses their Facebook account from the same web browser.  
 21 “Cookies are small files of information that a web server generates and sends to a web browser.”  
 “Cookies help inform websites about the user, enabling the websites to personalize the user  
 experience.” What are Cookies?, <https://www.cloudflare.com/learning/privacy/what-are-cookies/>  
 22 (last visited Jan. 27, 2023).

23 <sup>22</sup> “CAPI works with your Meta Pixel to help improve the performance and measurement of your  
 Facebook ad campaigns.” See Samir El Kamouny, How to Implement Facebook Conversions  
 API (In Shopify), FETCH & FUNNEL <https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited Jan. 25, 2023).

1           13. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to  
2 transmit information to Facebook in addition to the website owner, CAPI does not cause the user's  
3 browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website  
4 interaction, including Private Information, records and stores that information on the website  
5 owner's servers, and then transmits the data to Facebook from the website owner's servers.<sup>23, 24</sup>

6           14. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and  
7 attribution across your customer's full journey, from discovery to conversion. This helps you better  
8 understand how digital advertising impacts both online and offline results."<sup>25</sup>

9           15. Because CAPI is located on the website owner's servers and is not a bug planted  
10 onto the website user's browser, it allows website owners like Defendant to circumvent any ad  
11 blockers or other denials of consent by the website user that would prevent the Meta Pixel from  
12 sending website users' Private Information to Facebook directly.

13           16. Defendant utilized data from these trackers to market its services and bolster its  
14 profits. Meta Pixel and CAPI are routinely used to target specific customers by utilizing data to  
15 build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's  
16 and Class Members' Private Information to create targeted advertisements based on the medical  
17 conditions and other information disclosed to Defendant.

18           17. The information that Defendant's Meta Pixel and possibly CAPI sent to Facebook  
19

---

20           <sup>23</sup> What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG,  
21 <https://revealbot.com/blog/facebook-conversions-api/> (last updated May 20, 2022).

22           <sup>24</sup> "Server events are linked to a dataset ID and are processed like events sent via the Meta  
Pixel.... This means that server events may be used in measurement, reporting, or optimization  
in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS,  
23 <https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited May 15, 2023).

<sup>25</sup> About Conversions API, META FOR DEVELOPERS,  
<https://www.facebook.com/business/help/2041148702652965> (last visited May 15, 2023).

1 can include the Private Information that Plaintiff and Class Members submitted to Defendant's  
2 Website, including details about the pages they browsed and the buttons they clicked, including,  
3 (i) users' keyword searches, (ii) users' physician searches, (iii) content that users viewed;  
4 (iv) activities that reveal the users' status as potential patients; and (v) identifying information.

5 18. Such information allows a third party (e.g., Facebook) to know that a specific  
6 patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class  
7 Members' Private Information to third-party marketers, who then geotarget Plaintiff's and Class  
8 Members' Facebook pages based on communications obtained via the Meta Pixel and CAPI.  
9 Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information  
10 also could reasonably infer from the data that a specific patient was being treated for a specific  
11 type of medical condition, such as cancer, pregnancy, dementia, or HIV.

12 19. In addition to the Facebook tracker and CAPI, on information and belief, Defendant  
13 installed other tracking technology which operate similarly to the Meta Pixel and transmit a  
14 website user's Private Information to other third parties.

15 20. Healthcare patients simply do not anticipate that their trusted healthcare provider  
16 will send Personal Health Information ("PHI") or other confidential medical information collected  
17 via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy  
18 violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

19 21. Neither Plaintiff nor any Class Member signed a written authorization permitting  
20 Defendant to send their Private Information to Facebook, or any other third parties uninvolved in  
21 their treatment.

22 22. Despite willfully and intentionally incorporating tracking technology, including the  
23 Meta Pixel, potentially CAPI, and other tracking technology such as Google Analytics with Google

1 Tag Manager ("GTM"), Facebook Events, AppDynamics, Taboola, Pinterest, StackAdapt,  
2 LinkedIn, DoubleClick, Skai, Microsoft Universal Events, and Medallia, into its Website and  
3 servers, Banner has never disclosed to Plaintiff or Class Members that it shared their sensitive and  
4 confidential communications and Private Information with third parties including Facebook, and  
5 potentially others.

6 23. Defendant further made express and implied promises to protect Plaintiff's and  
7 Class Members' Private Information and maintain the privacy and confidentiality of  
8 communications that patients exchanged with Defendant, including in its privacy policies and  
9 elsewhere.

10 24. Defendant owed common law, statutory, and regulatory duties to keep Plaintiff's  
11 and Class Members' communications and Private Information safe, secure, and confidential.

12 25. Upon information and belief, Banner utilized the Meta Pixel and other tracker data  
13 to improve and to save costs on its marketing campaigns, improve its data analytics, attract new  
14 patients, and generate sales.

15 26. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff's  
16 and Class Members' Private Information, Defendant assumed legal and equitable duties to those  
17 individuals to protect and to safeguard that information from unauthorized disclosure.

18 27. Defendant breached its statutory and common law obligations to Plaintiff and Class  
19 Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based  
20 technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage  
21 technology that was known and designed to share web-users' information; (iii) aiding, agreeing,  
22 and conspiring with third parties to intercept communications sent and received by Plaintiff and  
23 Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to

1 disclose their Private Information to Facebook and others; (v) failing to protect Private Information  
2 and take steps to block the transmission of Plaintiff's and Class Members' Private Information  
3 through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class  
4 Members; and (vii) otherwise failing to design and monitor its Website to maintain the  
5 confidentiality and integrity of patient Private Information.

6 28. Plaintiff seeks to remedy these harms and brings causes of action for  
7 (I) Negligence; (II) Breach of Implied Contract; (III) Unjust Enrichment; (IV) Breach of Fiduciary  
8 Duty; (V) Invasion of Privacy; (VI) Invasion of Privacy under the California Constitution, Cal.  
9 Const. ART. 1 § 1; (VII) Violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal  
10 Code §§ 630, *et seq.*; (VIII) Violation of the California Confidentiality of Medical Information  
11 Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, 56.101; (IX) Violation of the Comprehensive  
12 Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and, (X) Violation of  
13 Cal. Bus. & Prof. Code §§ 17200, *et seq.*

#### 14 PARTIES

15 29. Plaintiff, JOHN DOE, is a natural person and a resident and citizen of the State of  
16 California where he intends to remain, with a principal residence in Susanville, California in  
17 Lassen County. He is a patient of Defendant and a victim of Banner's Disclosure of his Private  
18 Information.

19 30. Defendant, BANNER HEALTH ("Banner" or "Defendant"), is a not-for-profit  
20 corporation organized and existing under the laws of the State of Arizona with its principal place  
21 of business at 2901 North Central Avenue, Suite 160, Phoenix, Arizona 85012 in Maricopa  
22 County.

23 31. Defendant's Registered Agent for Service of Process is C T Corporation System,

330 N Brand Boulevard, Suite 700, Glendale, California 91203.

## JURISDICTION & VENUE

32. The Court has personal jurisdiction over Defendant because Banner transacts business in the State of California by providing medical treatment services.

33. This is a class action brought pursuant to Cal. Civ. Proc. Code § 382, and this Court has jurisdiction over the Plaintiff's claims because the amount in controversy exceeds this Court's jurisdictional minimum.

34. Venue is proper under Cal. Civ. Proc. Code § 395(a) because the injury to personal property complained of herein occurred in Lassen County.

## COMMON FACTUAL ALLEGATIONS

### A. Background

35. Founded in 1999 and based on Pheonix, Arizona, Banner is a massive healthcare system which provides treatment services to patients in Arizona, California, Colorado, Nebraska Nevada, Wyoming,<sup>26</sup> and in Alaska, through "28 hospitals and a growing network of health centers and clinics."<sup>27</sup>

36. On its Website, Defendant represents to patients and prospective patients that:

At all stages in life, you can rest assured that Banner will meet your health and medical needs through compassionate professionals and outstanding service. Headquartered in Phoenix, Arizona., Banner Health is one of the largest, nonprofit health care systems in the country and the leading nonprofit provider of hospital services in all the communities we serve.<sup>28</sup>

37. Indeed, Banner owns and operates numerous hospital and medical centers, including: Banner Boswell Medical Center in Sun City, Arizona; Banner Del E Webb Medical

---

<sup>26</sup> See generally, <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

<sup>27</sup> <https://www.bannerhealth.com/about/glance/history> (last acc. Mar. 8, 2024).

<sup>28</sup> <https://www.bannerhealth.com/about> (last acc. Mar. 8, 2024).

Center, in Sun City West Arizona; Banner MD Anderson Cancer Center at Banner Gateway Medical Center, in Gilbert, Arizona; Banner Gateway Medical Center in Gilbert, Arizona; Banner Rehabilitation Hospital West in Peoria, Arizona; Banner Ocotillo Medical Center in Chandler, Arizona; Banner Behavioral Health Hospital in Scottsdale, Arizona; Banner - University Medical Center South in Tucson, Arizona; Banner - University Medical Center Tucson in Tucson, Arizona; Diamond Children's Medical Center in Tucson, Arizona; Banner Thunderbird Medical Center and Banner Children's at Thunderbird in Glendale, Arizona; Banner Payson Medical Center in Payson, Arizona; Banner Children's at Desert in Mesa, Arizona; Banner Desert Medical Center in Mesa, Arizona; Banner Heart Hospital in Mesa, Arizona; Banner Rehabilitation Hospital East and Banner Baywood Medical Center in Mesa, Arizona; Banner Ironwood Medical Center in Queen Creek, Arizona; Banner Goldfield Medical Center in Apache Junction, Arizona; Banner Rehabilitation Hospital Phoenix, Banner Estrella Medical Center, and Banner - University Medical Center Phoenix in Phoenix, Arizona; Page Hospital in Page, Arizona; Banner Lassen Medical Center in Susanville, California; Banner Casa Grande Medical Center in Casa Grande, Arizona; Sterling Regional MedCenter in Sterling, Colorado; Banner Fort Collins Medical Center in Fort Collins, Colorado; Banner North Colorado Medical Center in Greeley, Colorado; East Morgan County Hospital in Brush, Colorado; Banner McKee Medical Center in Loveland, Colorado; Banner Churchill Community Hospital in Fallon, Nevada; Community Hospital in Torrington, Wyoming; Banner Wyoming Medical Center in Casper, Wyoming; Platte County Memorial Hospital in Wheatland, Wyoming; Washakie Medical Center in Worland, Wyoming; Ogallala Community Hospital in Ogallala, Nebraska.<sup>29</sup>

---

<sup>29</sup> See, "Locations," avail. at <https://www.bannerhealth.com/locations?loctype=Hospital&PageNo=1> (last acc. Mar. 8, 2024).



1           38. One of these facilities is Banner Lassen Medical Center in Susanville, California,  
 2 originally founded in 1883, “[a] 25-bed, critical access hospital” with a “focus [] to provide you  
 3 with outstanding care and an excellent patient care experience through the latest in medical  
 4 technology, a vision of compassion, and a concentration on patient and employee safety [...and...]  
 5 offer[ing] a wide range of programs and services to aid in prevention, diagnosis and treatment of  
 6 illness.”<sup>30</sup>

7           39. Another one of Defendant’s facilities is University Medical Center Tucson,  
 8 established in 1971, a “non-profit hospital with 649 licensed beds, providing a wide range of  
 9 inpatient and outpatient services [with] more than 3,000 health care professionals and support staff,  
 10 and a medical staff of more than 1,300 physicians who serve Tucson and surrounding areas.”<sup>31</sup>

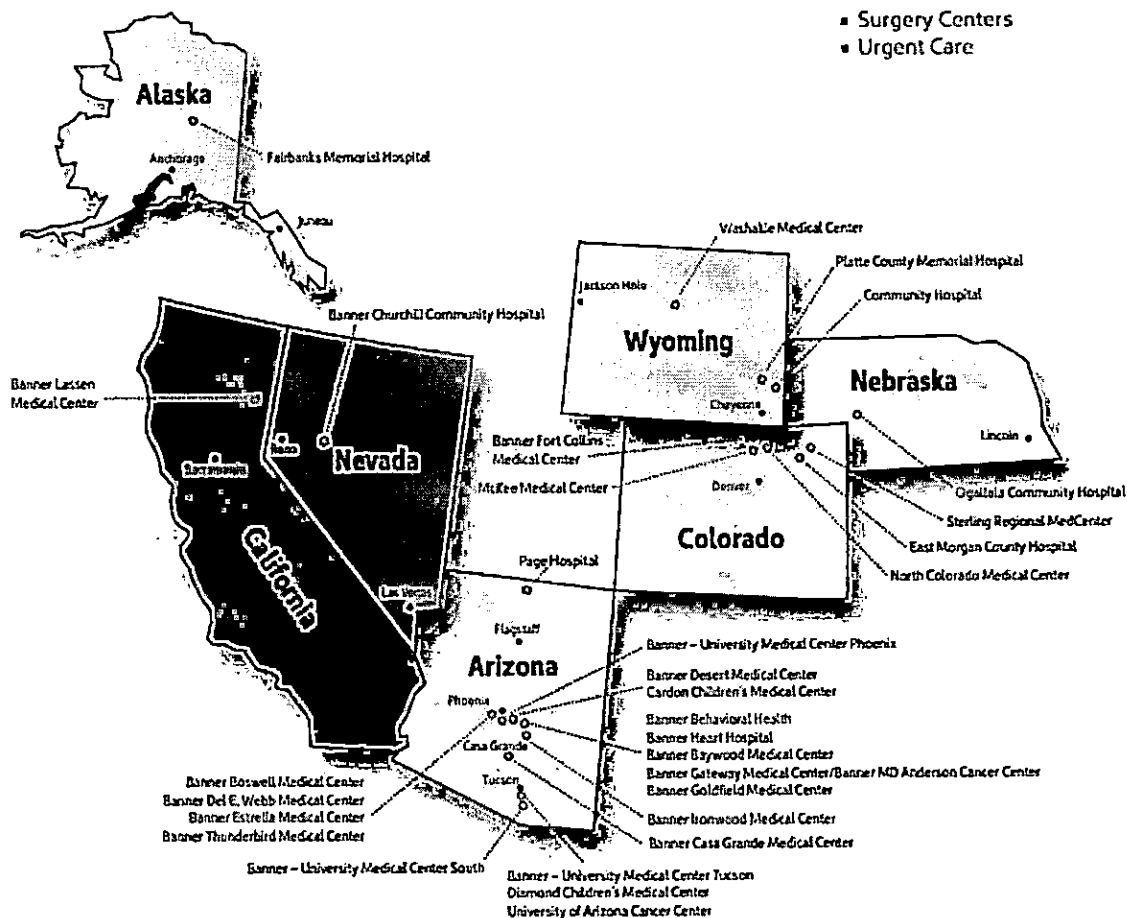
11           40. Moreover, banner operates hundreds of physicians’ clinics, urgent care clinics,  
 12 diagnostic imaging practices, physical therapy locations, surgery centers, specialized breast health  
 13 centers, emergency care departments, as well as home care and equipment locations, laboratories,  
 14 pharmacies, specialty care centers (e.g., Banner MD Anderson Cancer Center), and other health  
 15 service locations such as Banner Health schools and senior centers.<sup>32</sup>

20 <sup>30</sup> <https://www.bannerhealth.com/locations/susanville/banner-lassen-medical-center> (last acc.  
 21 Mar. 12, 2024).

22 <sup>31</sup> *Banner Health 2022 CHNA Banner University Medical Center – Tucson Banner University*  
 23 *Medical Center – South*, adopted by Banner Health Board of Directors Dec. 9, 2022, pg. 1, avail.  
 at <https://www.bannerhealth.com/-/media/files/project/bh/chna-reports/2022/arizona/banner-university-medical-centers-tucson-and-south-cover-section-tucson.ashx#:~:text=On%20an%20annual%20basis%2C%20Banner.65%2C000%20patients%20in%20the%20ED> (last acc. Mar. 8, 2024).

<sup>32</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

41. As shown on its Website, the scope of Banner's treatment is truly nationwide:<sup>33</sup>



42. At its many medical care facilities, Banner provides myriad medical treatment services, including in areas of: emergency medical care; surgery (including outpatient surgery, general surgery, and neurosurgery); Academic Medicine; Allergy & Immunology; Alzheimer's Disease & Dementia; Asthma; Audiology; Banner Brain & Spine; Bariatric & Weight Loss Surgery; Behavioral & Mental Health; Burn Care; Cancer; Concierge Medicine; Concussion; Critical Care Medicine; Dermatology; Diabetes; Doctors & Specialists; Ear, Nose & Throat;

<sup>33</sup> Banner Health, Fact Sheet, *A leading health care system in the nation*, avail. at <https://www.bannerhealth.com/-/media/files/project/bh/about/history/154267bhgeneralmainfs5115.ashx> (last acc. Mar. 8, 2024).

1 Endocrinology; Endoscopy; Eye Care; Family Medicine; Gastroenterology; Geriatrics;  
 2 Gynecology; Healthy Aging; Heart; Home Care; Hospice; Imaging; Infectious Disease; Infusion  
 3 Therapy; Injury Prevention; Integrative Therapy; Intensive Care; Internal Medicine; Kidney; Labs;  
 4 Maternity; Medical Imaging; Neonatology; Neurology; Nutrition; Obstetrics; Occupational  
 5 Health; Orthopedics; Pain Management; Palliative Care; Pediatrics; Pharmacy; Physical Therapy;  
 6 Poison & Drug Information Center; Primary Care; Psychology; Pulmonary; Rehabilitation;  
 7 Research; Spine; Sleep Medicine; Sports Medicine; Telehealth; Transplant; Urgent Care; Urology;  
 8 Women's Health; and Wound Care.<sup>34</sup>

9 43. Further, Banner provides specialized treatment through dedicated institutes,  
 10 including: Banner - University Medicine Heart Institute (“[t]he most current and advanced care  
 11 for your heart” with a Cardiovascular Intervention Center, Heart Rhythm Disorders Center, and  
 12 Women's Heart Center); Banner - University Medicine Neuroscience Institute (“State-of-the-art  
 13 care for neurological conditions”); Banner - University Orthopedic and Sports Medicine Institute  
 14 (“[e]xpert care to keep your muscles and joints moving”); and Banner - University Medicine  
 15 Women's Institute (“[c]omprehensive care from maternity to menopause”).<sup>35</sup>

16 44. Banner boasts having over 50,000 employees, being “one of the country's largest  
 17 employers [...], [ Arizona's...] largest private employer, and [] one of Northern Colorado's largest  
 18 employers.”<sup>36</sup>

19 45. Defendant touts that:

20 Ultimately, Banner's unwavering commitment to the health and well-being of its  
 21 communities has earned accolades from an array of industry organizations, Banner  
 22 Health's Supply Chain was recognized as second in the nation in 2021, and one of  
 the nation's Top 10 Integrated Health Systems according to SDI and Modern

23 <sup>34</sup> <https://www.bannerhealth.com/services/service-listing> (last acc. Mar. 8, 2024).

<sup>35</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

<sup>36</sup> <https://www.bannerhealth.com/about> (last acc. Mar. 8, 2024).

1 Healthcare Magazine. Banner Alzheimer's Institute has also garnered international  
2 recognition for its groundbreaking Alzheimer's Prevention Initiative, brain imaging  
3 research and patient care programs. Further, Banner Health, which is the second  
largest private employer in both Arizona and Northern Colorado, continues to be  
4 recognized as one of the "Best Places to Work" by Becker's Hospital Review.<sup>37</sup>

46. In 2023, Defendant generated annual revenue approximating \$7.8 billion.<sup>38</sup>

47. Banner serves many of its patients via its Online Platforms, which it encourages  
6 patients to use to learn about Banner on its main homepage,<sup>39</sup> to search for health information,<sup>40</sup>  
7 to find a doctor,<sup>41</sup> to find locations,<sup>42</sup> to learn about medical conditions and treatment services,<sup>43</sup>  
8 to learn about classes and events,<sup>44</sup> to access a patient portal,<sup>45</sup> to pay bills,<sup>46</sup> and more.

48. In furtherance of its goal of increasing sales and profitability, and to improve the  
10 success of its advertising and marketing, Defendant purposely installed the Meta Pixel and other  
11 trackers, such as Google Analytics with Google Tag Manager ("GTM"), Facebook Events,  
12 AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal  
13 Events, and Medallia onto its Website, for the purpose of gathering information about Plaintiff and  
14 Class Members to further its marketing efforts. But Defendant did not only generate information

16 <sup>37</sup> *Banner Health 2022 CHNA Banner University Medical Center – Tucson Banner University*  
17 *Medical Center – South*, adopted by Banner Health Board of Directors Dec. 9, 2022, pg. 1, avail.  
18 at <https://www.bannerhealth.com/-/media/files/project/bh/chna-reports/2022/arizona/banner-university-medical-centers-tucson-and-south-cover-section-tucson.ashx#:~:text=On%20an%20annual%20basis%2C%20Banner.65%2C000%20patients%20in%20the%20ED> (last acc. Mar. 8, 2024).

19 <sup>38</sup> <https://www.zippia.com/banner-health-careers-61932/revenue/> (last acc. Mar. 8, 2024).

20 <sup>39</sup> <https://www.bannerhealth.com/> (last acc. Mar. 8, 2024).

21 <sup>40</sup> E.g., search for "chest pain," avail. at  
<https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

22 <sup>41</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

23 <sup>42</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

<sup>43</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

<sup>44</sup> <https://www.bannerhealth.com/calendar> (last acc. Mar. 8, 2024).

<sup>45</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).

<sup>46</sup> <https://bannerhealth.simplepay.com/app/login> (last acc. Mar. 8, 2024).

1 for its own use: it also shared patient information, including Private Information belonging to  
 2 Plaintiff and Class Members, with Facebook and other unauthorized third parties.

3 49. To better understand Defendant's unlawful data-sharing practices, a brief  
 4 discussion of basic web design and tracking tools follows.

5 *i. Facebook's Business Tools and the Meta Pixel*

6 50. Facebook operates the world's largest social media company and generated \$117  
 7 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.<sup>47</sup>

8 51. In conjunction with its advertising business, Facebook encourages and promotes  
 9 entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify,  
 10 target, and market products and services to individuals.

11 52. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits  
 12 of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby  
 13 enabling the interception and collection of user activity on those platforms.

14 53. The Business Tools are automatically configured to capture "Standard Events" such  
 15 as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"),  
 16 as well as metadata, button clicks, and other information.<sup>48</sup> Businesses that want to target  
 17 customers and advertise their services, such as Defendant, can track other user actions and can  
 18

19  
 20 <sup>47</sup> Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK  
<https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Nov. 14, 2022).

21 <sup>48</sup> Specifications for Facebook Pixel Standard Events, META,  
<https://www.facebook.com/business/help/402791146561655> (last visited Jan. 31, 2023); *see also*  
 22 Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS;  
<https://developers.facebook.com/docs/facebook-pixel/advanced/>; *see also* Best Practices for  
 23 Facebook Pixel Setup, META <https://www.facebook.com/business/help/218844828315224>; App  
 Events API, META FOR DEVELOPERS, [https://developers.facebook.com/docs/marketing-api/app-](https://developers.facebook.com/docs/marketing-api/app-event-api/)  
 event-api/ (last visited Jan. 31, 2023).

1 create their own tracking parameters by building a “custom event.”<sup>49</sup>

2 54. One such Business Tool is the Meta Pixel, a tool that “tracks the people and type  
3 of actions they take.”<sup>50</sup> When a user accesses a webpage that is hosting the Meta Pixel, the  
4 communications with the host webpage are instantaneously and surreptitiously duplicated and sent  
5 to Facebook—traveling from the user’s browser to Facebook’s server.

6 55. Notably, this transmission only occurs on webpages that contain the Pixel. A  
7 website owner can configure its website to use the Pixel on certain webpages that don’t implicate  
8 patient privacy (such as the homepage) and disable it on pages that do implicate patient privacy  
9 (such as Defendant’s “Services” pages<sup>51</sup>).

10 56. The Meta Pixel’s primary purpose is for marketing and ad targeting and sales  
11 generation.<sup>52</sup>

12 57. Facebook’s own website informs companies that “[t]he Meta Pixel is a piece of  
13 code that you put on your website that allows you to measure the effectiveness of your advertising  
14 by understanding the actions people take on your website.”<sup>53</sup>

15 58. According to Facebook, the Meta Pixel can collect the following data.

16 **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard  
17 web protocol sent between any browser request and any server on the internet.  
18 HTTP Headers include IP addresses, information about the web browser, page  
location, document, referrer and *person using the website*. (emphasis added).

19 **Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.

20 <sup>49</sup> About Standard and Custom Website Events, META,  
21 <https://www.facebook.com/business/help/964258670337005>; *see also* Facebook, App Events  
API, *supra*.

22 <sup>50</sup> Retargeting, META, <https://www.facebook.com/business/goals/retargeting>.

23 <sup>51</sup> <https://pamhealth.com/health-services> (last acc. Mar. 6, 2024).

<sup>52</sup> *See* Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/>  
(last accessed Mar. 19, 2023).

<sup>53</sup> About Meta Pixel, META,  
<https://www.facebook.com/business/help/742478679120153> (last accessed Mar. 19, 2023).

1 **Button Click Data** – Includes any buttons clicked by site visitors, the labels those  
2 buttons and any pages visited as a result of the button clicks.

3 **Optional Values** – Developers and marketers can optionally choose to send  
4 additional information about the visit through Custom Data events. Example  
5 custom data events are conversion value, page type and more.

6 **Form Field Names** – Includes website field names like email, address, quantity,  
7 etc., for when you purchase a product or service. We don't capture field values  
8 unless you include them as part of Advanced Matching or optional values.<sup>54</sup>

9 59. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- 10 • **Make sure your ads are shown to the right people.** Find new customers,  
11 or people who have visited a specific page or taken a desired action on your  
12 website.
- 13 • **Drive more sales.** Set up automatic bidding to reach people who are more  
14 likely to take an action you care about, like making a purchase.
- 15 • **Measure the results of your ads.** Better understand the impact of your ads  
16 by measuring what happens when people see them.<sup>55</sup>

17 60. Facebook likewise benefits from the data received from the Meta Pixel and uses the  
18 data to serve targeted ads and identify users to be included in such targeted ads.

19 *ii. Defendant's method of transmitting Plaintiff's and Class Members' Private*  
20 *Information via the Meta Pixel and/or Conversions API i.e., the Interplay between*  
21 *HTTP Requests and Responses, Source Code, and the Meta Pixel*

22 61. Web browsers are software applications that allow consumers to navigate the  
23 internet and view and exchange electronic information and communications. Each "client device"  
(such as computer, tablet, or smart phone) accesses web content through a web browser (e.g.,  
Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's  
Edge browser).

<sup>54</sup> Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/> (last accessed Mar. 19, 2023).

<sup>55</sup> About Meta Pixel, META, <https://www.facebook.com/business/help/742478679120153> (last accessed Mar. 19, 2023).



1           62. Every website is hosted by a computer “server” that holds the website’s contents  
2 and through which the website owner exchanges files or communications with Internet users’  
3 client devices via their web browsers.

4           63. Web communications consist of HTTP Requests and HTTP Responses, and any  
5 given browsing session may consist of thousands of individual HTTP Requests and HTTP  
6 Responses, along with corresponding cookies.<sup>56</sup>

7           64. GET Requests are one of the most common types of HTTP Requests. In addition  
8 to specifying a particular URL (i.e., web address), they also send the host server data, which is  
9 embedded inside the URL and can include cookies.

10          65. When an individual visits a website, their web browser sends an HTTP Request to  
11 the entity’s servers that essentially asks the website to retrieve certain information (such as  
12 Defendant’s search function page). The entity’s servers send the HTTP Response, which contains  
13 the requested information in the form of “Markup.” This is the foundation for the pages, images,  
14 words, buttons, and other features that appear on the patient’s screen as they navigate a website.

15          66. Every website is comprised of Markup and “Source Code.” Source Code is simply  
16 a set of instructions that commands the website visitor’s browser to take certain actions when the  
17 web page first loads or when a specified event triggers the code.

18          67. Source code may also command a web browser to send data transmissions to third  
19 parties in the form of HTTP Requests quietly executed in the background without notifying the  
20 web browser’s user.

21  
22  
23 <sup>56</sup>“Cookies are small files of information that a web server generates and sends to a web browser . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience.” <https://www.cloudflare.com/learning/privacy/what-are-cookies/> (last visited Jan. 27, 2023).

1           68. Defendant's implementation of the Meta Pixel is source code that acted much like  
2 a traditional wiretap, intercepting and transmitting communications intended only for Defendant.

3           69. Separate from the Meta Pixel, Facebook and other website owners can place third-  
4 party cookies in the web browsers of users logged into their websites or services. These cookies  
5 can uniquely identify the user so the cookie owner can track the user as he moves around the  
6 internet—whether on the cookie owner's website or not. Facebook uses this type of third-party  
7 cookie when Facebook account holders use the Facebook app or website. As a result, when a  
8 Facebook account holder uses Defendant's Website, the account holder's unique Facebook ID is  
9 sent to Facebook, along with the intercepted communication, allowing Facebook to identify the  
10 patient associated with the Private Information it has intercepted.

11           70. With substantial work and technical know-how, internet users can sometimes  
12 circumvent this browser-based wiretap technology. To counteract this, third parties bent on  
13 gathering data and Private Information implement workarounds that are difficult to detect or evade.  
14 Facebook's workaround is its Conversions API tool, which is particularly effective because the  
15 data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the  
16 information travels directly from the entity's server to Facebook's server.

17           71. Conversions API "is designed to create a direct connection between [web hosts']  
18 marketing data and [Facebook]."<sup>57</sup> Thus, the entity receives and stores its communications with  
19 patients on its server before Conversions API collects and sends those communications—and the  
20 Private Information contained therein—to Facebook.

21           72. Notably, client devices do not have access to host servers and thus cannot prevent  
22  
23

---

<sup>57</sup> About Conversions API, META, <https://www.facebook.com/business/help/2041148702652965> (last visited May 15, 2023).

1 (or even detect) this additional transmission of information to Facebook.

2 73. While there is no way to confirm with certainty that a website owner is using  
3 Conversions API without accessing the host server, Facebook instructs companies like Defendant  
4 to “[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both  
5 tools,” because such a “redundant event setup” allows the entity “to share website events [with  
6 Facebook] that the pixel may lose.”<sup>58</sup> Thus, if an entity implemented the Meta Pixel in accordance  
7 with Facebook’s documentation, it is also reasonable to infer that it implemented the Conversions  
8 API tool on its Website.

9 74. The third parties to whom a website transmits data through pixels and other tracking  
10 technology do not provide any substantive content on the host website. In other words, Facebook  
11 and others like it are not providing anything to the user relating to the user’s communications.  
12 Instead, these third parties are typically procured to track user data and communications only to  
13 serve the marketing purposes of the website owner (i.e., to bolster profits).

14 75. Accordingly, without any knowledge, authorization, or action by a user, a website  
15 owner like Defendant can use its source code to commandeer its patients’ computing devices,  
16 causing the device’s web browser to contemporaneously and invisibly re-direct the patients’  
17 communications to hidden third parties like Facebook.

18 76. In this case, Defendant employed the Meta Pixel and potentially Conversions API  
19 to intercept, duplicate, and re-direct Plaintiff’s and Class Members’ Private Information to  
20 Facebook contemporaneously, invisibly, and without the patient’s knowledge.

21  
22  
23 

---

<sup>58</sup> See Best Practices for Conversions API, META,  
<https://www.facebook.com/business/help/308855623839366> (last visited May 15, 2023).

1           77. Consequently, when Plaintiff and Class Members visited Defendant's Website and  
2 communicated their Private Information, it was simultaneously intercepted and transmitted to  
3 Facebook.

4           78. On information and belief, Banner also employed other trackers, such Google  
5 Analytics with Google Tag Manager ("GTM"), Facebook Events, AppDynamics, Taboola,  
6 Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal Events, and Medallia,  
7 which likewise transmitted Plaintiff's and the Class Members' Private Information to third parties  
8 without Plaintiff's and Class Members' knowledge or authorization.

9           **iii. Defendant Violated its own Privacy Policies**

10           79. Banner maintains and is covered under privacy policies, including a Notice of  
11 Privacy Practices,<sup>59</sup> a Website Privacy Statement,<sup>60</sup> and a Website Terms of Use,<sup>61</sup> which are  
12 posted on Defendant's Website (collectively "Privacy Policies").

13           80. In its Notice of Privacy Practices, Defendant represents, acknowledges, and  
14 promises:

15           **Banner is committed to protecting the confidentiality of information about you**  
16 **and is required by law to do so.** This notice describes how we may use  
17 information about you within Banner Health and how we may disclose it to others  
18 outside Banner. **We will notify you if there is a breach of your unsecured**  
19 **protected health information.** This notice also describes the rights you have  
20 concerning your own health information.<sup>62</sup>

21 <sup>59</sup> Banner Health, *Notice of Privacy Practices*, effective date September 23, 2023, available at  
<https://www.bannerhealth.com/-/media/files/project/bh/patients-visitors/privacy-practices/hipaa-eng-fs-03-28-19.ashx> (last acc. Mar. 8, 2024), **attached as Exhibit B.**

22 <sup>60</sup> Banner Health, *Privacy Statement*, last updated November 2019, avail. at  
<https://www.bannerhealth.com/about/legal-notices/privacy> (last acc. Mar. 8, 2024), **attached as Exhibit C.**

23 <sup>61</sup> Banner Health, *Terms of Use*, avail. at <https://www.bannerhealth.com/about/legal-notices/terms> (last acc. Mar. 8, 2024), **attached as Exhibit D.**

<sup>62</sup> *Notice of Privacy Practices, Exhibit B* (emphases added).

1           81.     Therein, Banner further specifically represents, acknowledges, and promises that  
2 except as provided in the Notice of Privacy Practices, “[o]ther uses and disclosures not  
3 described in this notice will be made only with your written authorization, such as sale of  
4 medical information. You may revoke such an authorization by sending us a written request.”<sup>63</sup>

5           82.     Indeed, Banner’s Notice of Privacy Practices enumerates specific purposes for  
6 which it may disclose PHI/Private Information, including for: treatment (“Banner may use  
7 information about you to provide you with medical services and supplies. We may also disclose  
8 information about you to others that need the information to treat you, such as doctors, physician  
9 assistants, nurses, medical and nursing students, technicians, therapists, emergency service and  
10 medical transportation providers, medical equipment providers, and others involved in your  
11 care.”); in a Facility Directory; to family members and others involved in patient care; to effectuate  
12 payment for services; for health care operations (“Banner may use and disclose information about  
13 you if it is necessary to improve the quality of care we provide to patients or for health care  
14 operations. We may use information about you to conduct quality improvement activities, to obtain  
15 audit, accounting, or legal services, or to conduct business management and planning. For  
16 example, we may use medical information to review our treatment and services and to evaluate  
17 the performance of our staff in caring for you.”); for fundraising; for research; as required by law  
18 (“Federal, state, or local laws do not require patient consent to disclose information that is required  
19 to be reported. For instance, we are required to report child abuse and neglect, gunshot wounds,  
20 etc. Public policy has determined that these types of needs outweigh the patient’s right to privacy.  
21 Banner is also required to give information to the state workers’ compensation program for work-  
22 related injuries.”); for public health purposes; in limited circumstances for public safety; in

23  

---

<sup>63</sup> *Id.* (bold emphasis added).

1 connection with Health Oversight Activities; to coroners, medical examiners, and funeral  
2 directors; in connection with organ and tissue donations; for military veterans, national security,  
3 and other government purposes; and in judicial proceedings, subject to certain requirements.<sup>64</sup>

4 83. None of the above purposes enumerated in Banner's Notice of Privacy Practices,  
5 for which it may disclose patients' health information/PHI/Private Information without written  
6 authorization, include Defendant disclosing that information to third-parties uninvolved in their  
7 treatment for marketing purposes.

8 84. Further, Defendant maintains a Privacy Statement, applicable to its Website, in  
9 which Banner states is applicable:

10 ... to the information we collect from you when you use voice, mobile device and  
11 desktop Banner Health platforms, tools and applications, BannerHealth.com and  
12 other Banner Health websites (collectively the "Services"), how we use that  
13 information, and when we disclose it. It will also give you more information about  
14 how to manage the personal information that you provide to us through the  
15 Services. This statement applies only to information you provide to us online while  
16 visiting or using our Services. It does not apply to information we have obtained or  
17 may obtain offline through other traditional means.<sup>65</sup>

18 85. In its Website Privacy Statement, Banner explains the information it collects from  
19 the Online Platforms, including "Automatically Collected Information" or "information []  
20 automatically received and sometimes collected from you when you use the Services [...]  
21 includ[ing] some or all of the following items: the name of the domain and host from which you  
22 access the Internet, including the Internet protocol (IP) address of the computer you are using and  
23 the IP address of your Internet Service Provider; the type and version of Internet browser software  
you use and your operating system; the type and version of your media player(s); the date and time  
you access our Services, the length of your stay and the specific pages, images, video or forms that

---

<sup>64</sup> *Id.*

<sup>65</sup> *Privacy Statement, Exhibit C.*

1 you access while using the Services; the Internet address of the website from which you linked  
2 directly to our Services and, if applicable, the search engine that referred you and any search strings  
3 or phrases that you entered into the search engine to find the Services; and demographic  
4 information concerning the country of origin of your computer and the language(s) used by it.”<sup>66</sup>

5 86. Further, therein, Banner explains that it collects information via cookies, stating:

6 "Cookies" are small files or records that we place on your computer's hard drive to  
7 distinguish you from other visitors using the Services. The use of cookies is a  
8 standard practice among websites to collect or track information about your  
9 activities while using the Services. Some websites use persistent cookies, which are  
10 placed on your computer and remain there until you delete them. Others use  
11 temporary cookies, which expire after some period or become overwritten by other  
12 data. **Banner Health Services use "session cookies" which disappear from your  
13 computer after you have closed your Internet browser.**

14 Most people do not know that cookies are being placed on their computers when  
15 they use Banner Health Services or most other websites because browsers are  
16 typically set to accept cookies. You can choose to have your browser warn you  
17 every time a cookie is being sent to you or you can turn off cookie placements. If  
18 you refuse cookies, you can still use Banner Health Services, but your overall  
19 experience may be affected and some functionality may be reduced or  
20 unavailable.<sup>67</sup>

21 87. Lastly, in the Privacy Statement, Defendant explains that it collects information  
22 Website users actively submit when they “(i) submit a job application; (ii) make an online  
23 donation; (iii) sign up for a class or event conducted at one of our medical centers; (iv) send an e-  
mail message to us or otherwise provide online comments, criticisms, suggestions or feedback; (v)  
participate in a chat session; (vi) purchase merchandise from the Banner Store; (vii) reserve a spot  
or make an appointment at a Banner Health facility; or (viii) pre-register for a hospital procedure  
such as surgery.”<sup>68</sup>

---

23 <sup>66</sup> *Id.*

<sup>67</sup> *Id.* (bold emphasis added).

<sup>68</sup> *Id.*



1           88. In its Privacy Statement, Defendant specifically delineates how it uses and shares  
2 Private Information, *to wit*:

- 3           • To process, complete or otherwise act upon or respond to your  
4 request or reason for submitting that information;
- 5           • To register and/or verify you in connection with a service or feature  
6 that you are attempting to access or obtain;
- 7           • To communicate with you about your request or reason for  
8 submitting that information;
- 9           • To provide additional information to you about Banner Health and  
10 its services that we believe may interest you;
- 11           • To study and analyze the use of the information and features  
12 available on our Services; and
- 13           • To assist, when necessary, in protecting our rights or property,  
14 enforcing the provisions of our Privacy Statement and Terms of Use,  
15 and/or preventing harm to you or others.<sup>69</sup>

16           89. None of the above-described purposes enumerated in Banner's Privacy Statement  
17 include the disclosure of Private Information to third parties uninvolved in patients' treatment for  
18 marketing purposes, without their authorization, as occurred in the Disclosure.

19           90. Moreover, in its Privacy Statement, Defendant specifically represents,  
20 acknowledges, and promises that, "*We do not sell User Information to third parties.* And except  
21 where we otherwise obtain your express permission, we share your User Information with third  
22 parties only under the limited circumstances stated, including: credit card authorizations, "to  
23 process a particular request you have made, to complete a purchase order for merchandise and to  
deliver your purchase to you or to process a donation[;]" "[...]to conduct background checks,  
obtain credit reports, verify prior employment, check references and for any other lawful purpose  
that is in our judgment reasonably necessary to our interviewing and hiring process; "...in response  
to judicial or other governmental subpoenas, warrants and court orders served on Banner Health

---

<sup>69</sup> *Id.*

1 in accordance with their terms, or as otherwise required by applicable law[;]" "to protect our rights  
 2 or property, to enforce the provisions of our Privacy Statement and Terms of Use, and/or to prevent  
 3 harm to you or others[;]" "...if Banner Health or its business is sold or offered for sale to another  
 4 company or person(s), if a petition for relief under the United States Bankruptcy Laws is filed by  
 5 or against Banner Health, or if Banner Health becomes subject to an order of appointment of a  
 6 trustee or receiver[;]" and sharing user correspondence and information provided in user emails  
 7 "with employees, volunteers, representatives, or agents most capable of addressing your  
 8 correspondence" if users communicate via email.<sup>70</sup>

9 91. Nothing in Defendant's Website Privacy Statement discloses Banner's use of the  
 10 Meta Pixel or related tracking technology, and that users' and patients' Private Information will  
 11 be disclosed to third parties uninvolved in patient's treatment, without their authorization.

12 92. Finally, Defendant maintains a Website Terms of Use, which states, "[b]y  
 13 accessing, using or downloading in any way, without limitation, any materials from this Website  
 14 or merely browsing this Website, you agree to and are bound by these Terms of Use."<sup>71</sup>

15 93. Banner's Website Terms of Use provides:

16 **Banner Health respects the privacy of visitors to our Website. Please see**  
 17 **Banner Health's Privacy Statement relating to the collection and use of your**  
 18 **information. User acknowledges and agrees that this Privacy Statement,**  
 19 **including but not limited to the manner that Banner Health collects, uses and**  
 20 **discloses User's personally identifiable information, is incorporated and made**  
 21 **part of these Terms of Use. If User does not agree to Banner Health's Privacy**  
 22 **Statement, then User should not use this Website or submit or post any personally**  
 23 **identifiable information on this Website. Questions regarding privacy issues should**  
 be directed to Banner Health System Web Services.<sup>72</sup>

<sup>70</sup> *Id.* (italics in original).

<sup>71</sup> *Terms of Use, Exhibit D.*

<sup>72</sup> *Id.* (bold emphasis added).

1           94. In addition, in its Website Terms of Use, Banner “reserves the right to monitor all  
2 network traffic to this Website to identify and/or block unauthorized attempts or intrusions to  
3 upload or change information or cause damage to this Website in any fashion. Anyone using this  
4 Website expressly consents to such monitoring.”<sup>73</sup>

5           95. Nothing in the Website Terms of Use discloses Banner’s use of the Meta Pixel or  
6 related tracking technology, and that users’ and patients’ Private Information will be disclosed to  
7 third parties uninvolved in patient’s treatment, without their authorization.

8           96. Despite these express, specific representations and promises in its Privacy Policies,  
9 Banner does indeed transfer Private Information to third parties. Using the Meta Pixel, Defendant  
10 used and disclosed Plaintiff’s and Class Member’s Private Information and confidential  
11 communications to Facebook, and other unauthorized third parties, without written authorization,  
12 in violation of Banner’s Privacy Policies.

13           ***iv. Banner Unauthorizedly Disclosed Plaintiff’s and the Class’s Private Information***

14           97. Defendant disclosed Plaintiff’s and Class Members’ Private Information and  
15 confidential communications to third parties for marketing purposes, including Facebook, and  
16 potentially others, including Google Analytics with Google Tag Manager (“GTM”),  
17 AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, Skai, Microsoft Universal Events, and  
18 Medallia, without Plaintiff’s and Class Members’ authorization.

19           98. Through its use of the Meta Pixel, Banner disclosed to Facebook Plaintiff’s and  
20 Class Members’ Private Information communicated via its Website, including details about the  
21 pages they browsed and the buttons they clicked, including (i) users’ keyword searches, (ii) users’  
22 physician searches, (iii) content that users viewed, and (iv) activities that reveal the users’ status  
23

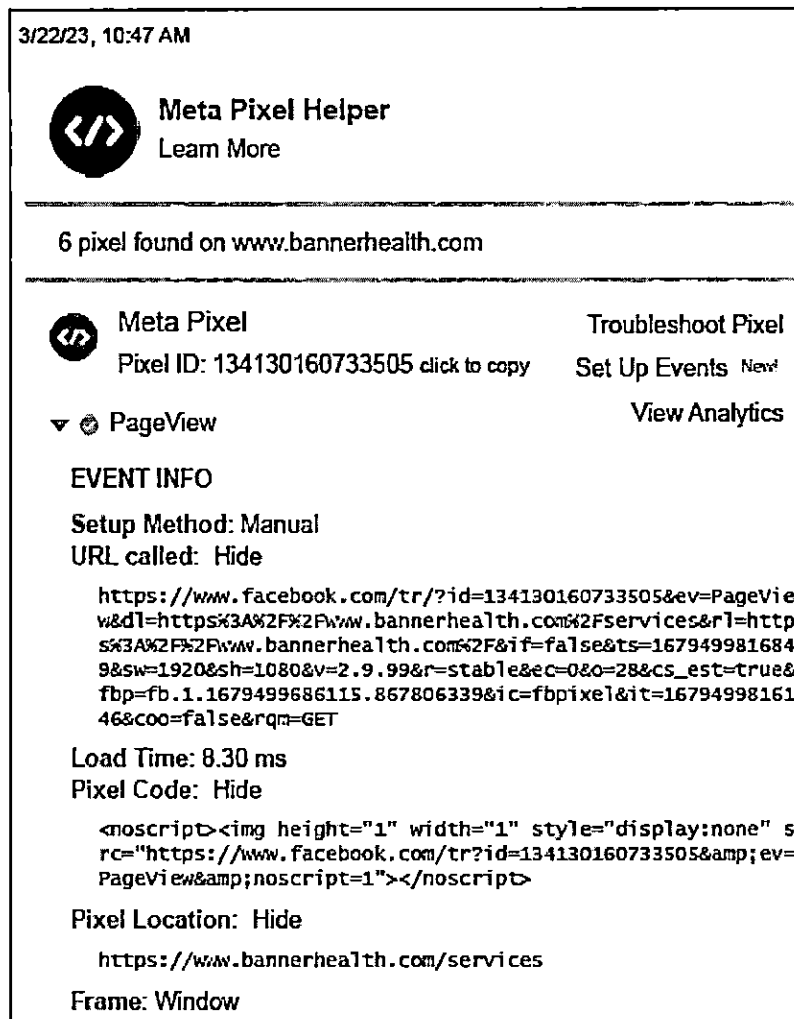
---

<sup>73</sup> *Id.*

as potential patients.

99. In addition to this information, (v) the Meta Pixel collects and transmits to Facebook other identifying information, including IP addresses, and users' "c\_user" cookies, which Facebook uses to identify users, and are transmitted in Meta Pixel events. Therefore, the Meta Pixel events Banner sent likely allowed Facebook to connect users' identities with the details reported within the events.

100. For example, Banner installed Meta Pixels on its pages for medical services:<sup>74</sup>



<sup>74</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

1 101. As of October 2023, Banner had multiple Meta Pixels installed on its Website with  
2 the following IDs: 534707753606264 (“Pixel1”); 354902315267014 (“Pixel2”);  
3 876783143355083 (“Pixel3”); 317691905318614 (“Pixel4”); 134130160733505 (“Pixel5”); and  
4 352572695583032 (“Pixel6”).

5 102. Even prior to that time, as of March 30, 2021, Banner had three additional Meta  
6 Pixels with IDs: 200525233628970 (“Pixel7”); 375127919853316 (“Pixel8”); and (9)  
7 499798837564477 (“Pixel9”). Further, there are three GTM accounts with IDs GTM-P6NQWFD  
8 (“GTM1”), GTM-K8Z9P6T (“GTM2”), and GTM-NSPWG36 (“GTM3”).

9 Banner Disclosed Users’ Keyword Searches

10 103. Banner shared information with Facebook about users’ searches through  
11 PageView, Microdata, and SubscribedButtonClick events.

12 104. Upon users’ arrival on Banner’s homepage, Banner sent PageView and Microdata  
13 events informing Facebook that the user was on “.” The Microdata event also provides that Banner  
14 offers healthcare in “AZ, CO, WY, NE, NV, CA” and that the user can “Find a provider, schedule  
15 an appointment, or find the nearest Banner Health location near you.”

16 105. As users moved beyond the homepage, Banner continued to report users’ activities  
17 to Facebook.

18 106. If that was not bad enough, Defendant sent Facebook Plaintiff’s and the Class  
19 Members’ search query information. For example, when a user searched for the keyword “cancer,”  
20 Banner reported that activity to Facebook through SubscribedButtonClick, PageView and  
21 Microdata events, which all disclosed the user’s “query=cancer.”

22 107. The SubscribedButtonClick event includes additional information about the user’s  
23 specific activities, such as that the user clicked a button labeled “Search” connected to a form that

1 allows the user to “Search for doctors, locations, services, and more.”

2 108. With the search results displayed, the user may refine their search results by  
3 displaying the results by categories such as all results, locations results, or services results only.  
4 Banner also reported this type of activity. For example, if the user clicked to display all results,  
5 Banner sent a SubscribedButtonClick event, revealing that the user clicked on a button labeled  
6 “SERVICES” on a page titled “Banner Health Search Results” and that the user navigated to that  
7 page by searching “query=cancer.”

8 Banner Disclosed Users’ Physician Search Activities

9 109. Banner informed Facebook when users searched for physicians on the Banner  
10 website through SubscribedButtonClick, PageView, and Microdata events.

11 110. Banner sent a SubscribedButtonClick event as soon as a user navigated to Banner’s  
12 Find A Doctor page.

13 111. The SubscribedButtonClick disclosed that the user clicked a button labeled “Find a  
14 Doctor” and that the user navigated to the user’s current page after viewing a page on  
15 “<https://www.bannerhealth.com/services/cancer>.”

16 112. Upon the user loading the Find a Doctor page, Banner sent a pair of PageView and  
17 Microdata events, confirming that the user landed on the page with a “physician-directory” for the  
18 user to “Find a Doctor near you.”

19 113. Finally, as the user clicked to search for an oncology physician, Banner sent another  
20 SubscribedButtonClick event, informing Facebook that the user clicked “Search” to “Find a  
21 Doctor.”  
22  
23

Banner Disclosed Content That Users Viewed

114. Additionally, Defendant shared information as to the contents of its Website pages which Website users viewed. Banner disclosed information about content that users viewed through PageView, Microdata, and SubscribedButtonClick events.

115. For instance, when a user clicked to view “Classes + Events,” Banner reported that via a SubscribedButtonClick event. When the user arrived on Banner’s calendar page for its classes and events, Banner sent a pair of PageView and Microdata events, disclosing that the user was looking at the “/calendar” page.

116. Banner continued to share the user’s activities as the user clicked on specific classes. For instance, when the user clicked to view more about a diabetes class, Banner reported that the user clicked a button labeled “Dial Into Diabetes: Nutrition Basics and Medication Management- Virtual” while the user was on the “Calendar” page.

117. When the Dial Into Diabetes information page loaded, Banner sent another pair of PageView and Microdata events. The Microdata event reveals the user’s potential health insurance status due to the fact that the event indicates the user must be insured by “Banner Medicare Advantage (Dual, HMO, PPO) in order to register for the class.”

118. Additionally, the Microdata event reveals more information about the Dial Into Diabetes class too, including the time and date of the event, e.g., “11/01/2023, 10:00 am,” and the modality of the class via “Microsoft Teams Meeting.”

119. Then, Banner disclosed the user’s registration for the class through a series of SubscribedButtonClick, PageView, and Microdata events.

120. As another illustration of Banner’s disclosures of content that users viewed, Banner transmitted a series of SubscribedButtonClick, PageView, and Microdata events as the user took



1 a heart health risk assessment on Banner's website.

2 121. Banner began reporting about the user's health risk assessment activities when the  
3 user clicked to view Banner's offered health risk assessments. As the user clicked to browse the  
4 offered assessments, Banner sent a SubscribedButtonClick event.

5 122. When the page loaded, Banner then sent a pair of PageView and Microdata events,  
6 informing Facebook that the user can take "free health risk assessments" to "learn about your risk  
7 as well as stay informed about your health."

8 123. Next, when the user loaded a page for the heart health risk assessment, Banner  
9 transmitted PageView and Microdata events, revealing that the user was viewing a "Heart Age  
10 Test" which allows the user to "Estimate your risk of heart and blood vessel disease."

11 124. As the user clicked to start the assessment, progressed through each question, and  
12 then completed the assessment, Banner sent a mixture of SubscribedButtonClick, Pageview, and  
13 Microdata events sharing the user's progress with Facebook.

14 Banner Discloses Users' Activities That Reveal Their Status as Potential Patients

15 125. Further still, Banner discloses Users' activities that reveal their status as potential  
16 patients. Through PageView, Microdata, and SubscribedButtonClick events, Banner disclosed  
17 information about users' activities that reveal their status as potential patients.

18 126. For example, when the user clicked to access the Patient Account page, Banner sent  
19 a SubscribedButtonClick event disclosing that the user clicked a button labeled "Patient Account"  
20 on a page titled "Patients & Visitors | Banner Health." Banner further sent PageView and  
21 Microdata events, informing Facebook that the user was now on the Patient Account page, which  
22 "offers 24/7 online access to your health information."

23 127. From the Patient Account page, the user could either click to create a patient

1 account or click to sign into their patient account. Both activities triggered a  
2 SubscribedButtonClick event, disclosing that the user was on the “/patient-account” page and that,  
3 either, the user clicked a button for “Creating an Account” or to “Sign In,” respectively.

4 128. In addition to Banner sharing information with Facebook about users’ patient  
5 account-related activities, Banner also sent events with data about users’ activities related to  
6 medical records.

7 129. As a user navigated to Banner’s page for patients and then to a subpage for medical  
8 records, Banner sent a series of SubscribedButtonClick, PageView, and Microdata events  
9 informing Facebook about those activities. The Microdata events reveal information about the  
10 pages that the user was viewing. For example, the Microdata event associated with the Patient page  
11 reveal that the page the user was viewing offered “resources . . . to make your patient visit or stay  
12 at a Banner Health location as comfortable and successful as possible.”

13 130. Similarly, the Microdata event for the Medical Records page disclose that users  
14 “can request copies of your medical record information” from Banner.

15 131. Moreover, Banner also disclosed information about users’ interactions related to  
16 medical bills. Upon the user clicking a button to open and loading a page about payment options  
17 and other billing information, Banner sent SubscribedButtonClick, PageView, and Microdata  
18 events, disclosing that the user clicked on a button to access Banner’s “patients/billing” page where  
19 they could “Learn more about the financial assistance programs, pricing, insurance information,  
20 programs and policies available for you at Banner Health.”

21 132. From Banner’s Billing page, the user had the option to pay their bill for services  
22 received from Banner’s various service centers: (i) the imaging section, (ii) the surgery center,  
23 (iii) urgent care unit, or (iv) the Wyoming Medical Center.

1           133. As the user clicked to pay their bill for imaging services, surgery center services,  
2 urgent care services, or Wyoming Medical Center services, Banner sent a SubscribedButtonClick  
3 event informing Facebook that the user clicked on a button labeled “Imaging online payment,”  
4 “Surgery Center online payment,” “Urgent Care online payment,” or “Wyoming Medical Center  
5 online payment,” respectively.

6           134. After the pages for the different Banner service centers loaded, Banner also sent a  
7 pair of PageView and Microdata events, each of which revealed additional data about the pages  
8 that the user was viewing. For instance, the Microdata event sent for the surgery center page  
9 informed Facebook that the user was viewing a page that was “Your one-stop shop for all Banner  
10 Surgery Center payment processes.”

11           135. When the user proceeded to pay, for example, on the urgent care billing page,  
12 Banner disclosed that activity as well through a SubscribedButtonClick event.

13           136. Banner also disclosed when the user loaded the login page for Wyoming Medical  
14 Center through a PageView event.

15                           Banner Discloses Users’ Identifying Information

16           137. In addition, as noted, the Meta Pixel collects and transmits to Facebook other  
17 identifying information, including Users’ IP addresses, and users’ “c\_user” cookies, which  
18 Facebook uses to identify users.

19           138. Therefore, the Meta Pixel events Banner sent likely allowed Facebook to connect  
20 users’ identities with the details reported within the events.

21           139. After receiving this information from Defendant, Facebook processes it, analyzes  
22 it, and assimilates it into its own massive datasets, before selling access to this data in the form of  
23 targeted advertisements. Employing “Audiences”—subsections of individuals identified as

1 sharing common traits—Facebook promises the ability to “find the people most likely to respond  
2 to your ad.”<sup>75</sup> Advertisers can purchase the ability to target their ads based on a variety of criteria:  
3 “Core Audiences,” individuals who share a location, age, gender, and/or language;<sup>76</sup> “Custom  
4 Audiences,” individuals who have taken a certain action, such as visiting a website, using an app,  
5 or buying a product bought a product;<sup>77</sup> and/or “Lookalike Audiences,” groups of individuals who  
6 “resemble” a Custom Audience, and who, as Facebook promises, “are likely to be interested in  
7 your business because they’re similar to your best existing customers.”<sup>78</sup>

8 140. Google and other companies process data in a similar manner and use it to build  
9 marketing and other data profiles allowing for targeted advertising.

10 141. Defendant could have chosen not to use the Meta Pixel, or it could have configured  
11 it to limit the information that it communicated to third parties, but it did not. Instead, it  
12 intentionally selected and took advantage of the features and functionality of the Pixel that resulted  
13 in the Disclosure of Plaintiff’s and Class Members’ Private Information.

14 142. Along those same lines, Defendant could have chosen not to use other tracking  
15 technologies such as, Google Analytics with Google Tag Manager (“GTM”), Facebook Events,  
16 AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal  
17 Events, and Medallia to track Plaintiff and Class Members private communications and transmit  
18 that information to unauthorized third parties. It did so anyway, intentionally taking advantage of  
19 these trackers despite the harm to Plaintiff’s and Class Members’ privacy.

21 \_\_\_\_\_  
22 <sup>75</sup> Audience Ad Targeting, Meta, <https://www.facebook.com/business/ads/ad-targeting> (last  
23 visited Aug. 14, 2023).

<sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center,  
<https://www.facebook.com/business/help/465262276878947> (last visited Aug. 14, 2023).

1           143. Defendant used and disclosed Plaintiff's and Class Members' Private Information  
2 to Facebook, and possibly other third parties, for the purpose of marketing their services and  
3 increasing its profits.

4           144. On information and belief, Defendant shared, traded, or sold Plaintiff's and Class  
5 Members' Private Information with Facebook, and potentially other third parties, in exchange for  
6 improved targeting and marketing services.

7           145. Plaintiff and the Class Members never consented, agreed, authorized, or otherwise  
8 permitted Defendant Banner to intercept their communications or to use or disclose their Private  
9 Information for marketing purposes. Plaintiff and the Class were never provided with any written  
10 notice that Defendant disclosed its patients' Protected Health Information to Facebook and others,  
11 nor were they provided any means of opting out of such disclosures. Defendant nonetheless  
12 knowingly disclosed Plaintiff's and the Class's Protected Health Information to unauthorized  
13 entities.

14           146. Plaintiff and Class Members relied on Defendant to keep their Private Information  
15 confidential and securely maintained, to use this information for legitimate healthcare purposes  
16 only, and to make only authorized disclosures of this information.

17           147. Furthermore, Defendant actively misrepresented that it would preserve the security  
18 and privacy of Plaintiff's and Class Members' Private Information. In actuality, Defendant shared  
19 data about Plaintiff's and Class Members' activities on the Online Platforms alongside identifying  
20 details about the Plaintiff and Class Members, such as their IP addresses.

21           148. By law, Plaintiff and the Class Members are entitled to privacy in their Protected  
22 Health Information and confidential communications. Banner deprived Plaintiff and Class  
23 Members of their privacy rights when it (1) implemented a system that surreptitiously tracked,

1 recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally  
 2 Identifiable Information, and Protected Health Information; (2) disclosed patients' Private  
 3 Information to unauthorized, third-party eavesdroppers, including Facebook and possibly others;  
 4 and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and  
 5 without obtaining their express written consent.

#### 6 **B. Plaintiff's Experience**

7 149. Plaintiff has been a patient of Defendant since 2008, approximately, receiving  
 8 healthcare services from Banner and physicians in Banner's network, including for spinal  
 9 degeneration at Banner Lassen Medical Center in Susanville, California.

10 150. Plaintiff relied on Banner's Website and Online Platforms to communicate  
 11 confidential patient information, beginning in 2021 using personal computing devices in Lassen  
 12 County, and last in October 2023. Specifically, he used the Website's search function to search  
 13 for health information on spinal degeneration, and to search for physicians;<sup>79</sup> used the Website's  
 14 find a doctor function;<sup>80</sup> used the patient account and/or patient portal, including to make medical  
 15 appointments, check laboratory results, and make recurring payments of bills for services.<sup>81</sup>

16 151. Plaintiff accessed Defendant's Website and Online Platforms at Defendant's  
 17 direction and encouragement. Plaintiff reasonably expected that his communications with Banner  
 18 were confidential, solely between himself and Banner, and that, as such, those communications  
 19 would not be transmitted to or intercepted by a third party.

20 152. Plaintiff provided his Private Information to Defendant and trusted that the  
 21

22 <sup>79</sup> E.g., search for "chest pain," avail. at  
<https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

23 <sup>80</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

<sup>81</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).

1 information would be safeguarded according to Banner's Privacy Policies and the law.

2 153. On information and belief, through its use of the Meta Pixel on the Website and  
3 Online Platforms, Defendant disclosed to Facebook:

- 4 a. Plaintiff's identity via his IP addresses and/or "c\_user" cookies;
- 5 b. Plaintiff's seeking of medical treatment;
- 6 c. Plaintiff's status as a patient;
- 7 d. Plaintiff's search terms and activities, including relating to his health  
8 information and diagnoses, and doctors;
- 9 e. The doctors Plaintiff searched for and viewed;
- 10 f. The pages and content Plaintiff viewed; and,
- 11 g. Plaintiff's activity on the patient account and/or patient portal, including the  
12 appointments he scheduled, his laboratory results, and bills he paid.

13 154. By failing to receive the requisite consent, Banner breached confidentiality and  
14 unlawfully disclosed Plaintiff's Private Information.

15 155. Plaintiff first discovered that Defendant was using the Meta Pixel and other tracking  
16 technologies to gather and disclose his Private Information in October of 2023.

17 156. As a result of Banner's Disclosure of Plaintiff's Private Information via the Meta  
18 Pixel and other tracking technologies to third parties without authorization, Plaintiff now receives  
19 targeted health-related advertisements relating to spinal degeneration and having a newborn baby,  
20 reflecting his private medical treatment information.

21 157. Plaintiff paid Banner for medical services and the services he paid for included  
22 reasonable privacy and data security protections for his Private Information, but Plaintiff did not  
23 receive the privacy and security protections for which he paid, due to Defendant's Disclosure.



1           158. Because of Defendant's unauthorized Disclosure of his Private Information,  
2 Plaintiff has suffered injuries, including monetary damages; loss of privacy; unauthorized  
3 disclosure of this Private Information; unauthorized access to his Private Information by third  
4 parties; use of the Private Information for advertising purposes; embarrassment, humiliation,  
5 frustration, and emotional distress; decreased value of his Private Information; lost benefit of the  
6 bargain; and increased risk of future harm resulting from further unauthorized use and disclosure  
7 of his information.

8           **C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI**

9           159. In June 2020, after promising users that app developers would not have access to  
10 data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party  
11 developers to access this data.<sup>82</sup> This failure to protect users' data enabled thousands of developers  
12 to see data on inactive users' accounts if those users were Facebook friends with someone who  
13 was an active user.

14           160. On February 18, 2021, the New York State Department of Financial Services  
15 released a report detailing the significant privacy concerns associated with Facebook's data  
16 collection practices, including the collection of health data. The report noted that while Facebook  
17 maintained a policy that instructed developers not to transmit sensitive medical information,  
18 Facebook received, stored, and analyzed this information anyway. The report concluded that  
19 "[t]he information provided by Facebook has made it clear that Facebook's internal controls on  
20 this issue have been very limited and were not effective . . . at preventing the receipt of sensitive  
21  
22  
23

---

<sup>82</sup> Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) <https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/>.

1 data.”<sup>83</sup>

2 161. The New York State Department of Financial Service’s concern about Facebook’s  
3 cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a  
4 different settlement involving Facebook’s monetizing of sensitive medical data. In that case, the  
5 more than 100 million users of Flo, a period and ovulation tracking app, learned something  
6 startling: the company was sharing their data with Facebook.<sup>84</sup> When a user was having his period  
7 or informed the app of his intention to get pregnant, Flo would tell Facebook, which could then  
8 use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the  
9 Federal Trade Commission for lying to its users about secretly sharing their data with Facebook,  
10 as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and  
11 Flurry. The FTC reported that Flo “took no action to limit what these companies could do with  
12 users’ information.”<sup>85</sup>

13 162. More recently, Facebook employees admitted to lax protections for sensitive user  
14 data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that  
15 “[w]e do not have an adequate level of control and explainability over how our systems use data,  
16 and thus we can’t confidently make controlled policy changes or external commitments such as  
17 ‘we will not use X data for Y purpose.’”<sup>86</sup>

19  
20 <sup>83</sup> New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK  
INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021)  
[https://www.dfs.ny.gov/system/files/documents/2021/02/facebook\\_report\\_20210218.pdf](https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf).

21 <sup>84</sup> Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.)  
<https://slate.com/technology/2022/06/health-data-brokers-privacy.html>.

22 <sup>85</sup> *Id.*

23 <sup>86</sup> Lorenzo Franceschi-Bicchierai, Facebook Doesn’t Know What It Does with Your Data, or  
Where It Goes: Leaked Document, VICE (April 26, 2022)  
<https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes>.

1           163. Furthermore, in June 2022, an investigation by The Markup<sup>87</sup> revealed that the Meta  
 2 Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.<sup>88</sup> On those hospital  
 3 websites, the Meta Pixel collects and sends Facebook a “packet of data,” including sensitive  
 4 personal health information, whenever a user interacts with the website, for example, by clicking  
 5 a button to schedule a doctor’s appointment.<sup>89</sup> The data is connected to an IP address, which is “an  
 6 identifier that’s like a computer’s mailing address and can generally be linked to a specific  
 7 individual or household—creating an intimate receipt of the appointment request for Facebook.”<sup>90</sup>

8           164. During its investigation, The Markup found that Facebook’s purported “filtering”  
 9 failed to discard even the most obvious forms of sexual health information. Worse, the article  
 10 found that the data that the Meta Pixel was sending Facebook from hospital websites not only  
 11 included details such as patients’ medications, descriptions of their allergic reactions, details about  
 12 their upcoming doctor’s appointments, but also included patients’ names, addresses, email  
 13 addresses, and phone numbers.<sup>91</sup>

14           165. In addition to the 33 hospitals identified by The Markup that had installed the Meta  
 15 Pixel on their websites, The Markup identified seven health systems that had installed the Meta  
 16 Pixel inside their password-protected patient portals.<sup>92</sup>

17           166. David Holtzman, health privacy consultant and former senior privacy adviser in the  
 18

19  
 20 <sup>87</sup> The Markup is a nonprofit newsroom that investigates how powerful institutions are using  
 technology to change our society. See [www.themarkup.org/about](http://www.themarkup.org/about) (last accessed Mar. 19, 2023).

21 <sup>88</sup> Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving  
 Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.)  
 22 [https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-](https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites)  
[information-from-hospital-websites.](https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites)

23 <sup>89</sup> *Id.*

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

<sup>92</sup> *Id.*

1 U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply  
2 troubled" by what the hospitals capturing and sharing patient data in this way.<sup>93</sup>

### 3 **D. Defendant Violated HIPAA Standards**

4 167. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-  
5 public medical information (PHI) about a patient, a potential patient, or household member of a  
6 patient for marketing purposes without the patients' express written authorization.<sup>94</sup>

7 168. Guidance from the United States Department of Health and Human Services  
8 instructs healthcare providers that patient status alone is protected by HIPAA.

9 169. In Guidance regarding Methods for De-identification of Protected Health  
10 Information in Accordance with the Health Insurance Portability and Accountability Act Privacy  
11 Rule, the Department instructs:

12 Identifying information alone, such as personal names, residential addresses, or  
13 phone numbers, would not necessarily be designated as PHI. For instance, if such  
14 information was reported as part of a publicly accessible data source, such as a  
15 phone book, then this information would not be PHI because it is not related to  
16 health data... If such information was listed with health condition, health care  
17 provision, or payment data, such as an indication that the individual was treated at  
18 a certain clinic, then this information would be PHI.<sup>95</sup>

16 170. In its guidance for Marketing, the Department further instructs:

17 The HIPAA Privacy Rule gives individuals important controls over whether and  
18 how their protected health information is used and disclosed for marketing  
19 purposes. With limited exceptions, the Rule requires an individual's written  
20 authorization before a use or disclosure of his or his protected health information  
21 can be made for marketing. ... Simply put, a covered entity may not sell protected  
22 health information to a business associate or any other third party for that party's

---

21 <sup>93</sup> *Id.*

22 <sup>94</sup> HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

23 <sup>95</sup> U.S. Department of Health and Human Services, Guidance Regarding Methods for De-  
identification of Protected Health Information in Accordance with the Health Insurance  
Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012)  
[https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-  
identification/hhs\\_deid\\_guidance.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf).

own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).<sup>96</sup>

171. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates (“regulated entities”) under the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) when using online tracking technology.<sup>97</sup>

172. According to the Bulletin, “HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information.”<sup>98</sup>

173. Citing The Markup’s June 2022 article, the Bulletin expressly notes:

Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.

An impermissible disclosure of an individual’s PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual’s PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not

<sup>96</sup> U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf>.

<sup>97</sup> See U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, <https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html>.

<sup>98</sup> *Id.*

1 impermissibly disclose PHI to tracking technology vendors, because of the  
 2 proliferation of tracking technologies collecting sensitive information, now more  
 3 than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as  
 4 expressly permitted or required by the HIPAA Privacy Rule.<sup>99</sup>

5 174. In other words, HHS has expressly stated that Defendant's conduct of  
 6 implementing the Meta Pixel is a violation of HIPAA Rules.

7 **E. Defendant Violated FTC Standards, and the FTC and HHS Take Action**

8 175. The Federal Trade Commission ("FTC") has also recognized that implementation  
 9 of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and  
 10 "impermissibly disclos[e] consumers' sensitive personal health information to third parties."<sup>100</sup>

11 176. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130  
 12 hospital systems and telehealth providers to alert them about the risks and concerns about the use  
 13 of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online  
 14 activities."<sup>101</sup>

15 177. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are  
 16 not permitted to use tracking technologies in a manner that would result in impermissible  
 17 disclosures of PHI to third parties or any other violations of the HIPAA Rules"<sup>102</sup> and that "[t]his  
 18 is true even if you relied upon a third party to develop your website or mobile app and even if you  
 19 do not use the information obtained through use of a tracking technology for any marketing

20 <sup>99</sup> *Id.* (emphasis in original) (internal citations omitted).

21 <sup>100</sup> Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20,  
 22 2023) (available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf)), **Exhibit A**.

23 <sup>101</sup> FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security  
 Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023)  
[https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm\\_source=govdelivery](https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery).

<sup>102</sup> *Id.*

1 purposes.”<sup>103</sup>

2 178. Entities that are not covered by HIPAA also face accountability for disclosing  
 3 consumers’ sensitive health information under the Health Breach Notification Rule. 16 C.F.R. §  
 4 318. This Rule requires that companies dealing with health records notify the FTC and consumers  
 5 if there has been a breach of unsecured identifiable health information, or else face civil penalties  
 6 for violations. *Id.* According to the FTC, “a ‘breach’ is not limited to cybersecurity intrusions or  
 7 nefarious behavior. Incidents of unauthorized access, *including sharing of covered information*  
 8 *without an individual’s authorization*, triggers notification obligations under the Rule.”<sup>104</sup>

9 179. Additionally, the FTC Act makes it unlawful to employ “[u]nfair methods of  
 10 competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting  
 11 commerce[.]” 15 U.S.C. § 45(a). According to the FTC, “the disclosure of [sensitive health]  
 12 information without a consumer’s authorization can, in some circumstances, violate the FTC Act  
 13 as well as constitute a breach of security under the FTC’s Health Breach Notification Rule.”<sup>105</sup>

14 180. As such, the FTC and HHS have expressly stated that conduct like Defendant’s  
 15 runs afoul of the FTC Act and/or the FTC’s Health Breach Notification Rule.

---

18 <sup>103</sup> *Id.*

19 <sup>104</sup> Statement of the Commission: On Breaches by Health Apps and Other Connected Devices,  
 U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at  
 20 [https://www.ftc.gov/system/files/documents/public\\_statements/1596364/statement\\_of\\_the\\_commission\\_on\\_breaches\\_by\\_health\\_apps\\_and\\_other\\_connected\\_devices.pdf](https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf)) (emphasis added).

21 <sup>105</sup> *See, e.g.*, U.S. v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023),  
<https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v>;  
 22 In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (July 14, 2023),  
<https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter>; U.S.  
 23 v. GoodRx Holdings, Inc., Case No. 23-cv-460 (N.D. Cal. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc>; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), <https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc>.



**F. Defendant Violated Industry Standards**

181. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

182. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Banner and its physicians.

183. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

184. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

185. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

**G. Plaintiff's and Class Members' Expectation of Privacy**

186. At all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial

1 marketing and sales purposes, unrelated to patient care.

2 **H. IP Addresses are Personally Identifiable Information**

3 187. Defendant also disclosed and otherwise assisted Facebook and potentially others  
4 with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel and other  
5 tracking technologies.

6 188. An IP address is a number that identifies the address of a device connected to the  
7 Internet.

8 189. IP addresses are used to identify and route communications on the Internet.

9 190. IP addresses of individual Internet users are used by Internet service providers,  
10 Websites, and third-party tracking companies to facilitate and track Internet communications.

11 191. Facebook tracks every IP address ever associated with a Facebook user.

12 192. Facebook tracks IP addresses for use of targeting individual homes and their  
13 occupants with advertising.

14 193. Under HIPAA, an IP address is Personally Identifiable Information:

- 15 • HIPAA defines personally identifiable information to include "any unique  
16 identifying number, characteristic or code" and specifically lists the example of IP  
addresses. *See* 45 C.F.R. § 164.514 (2).
- 17 • HIPAA further declares information as personally identifiable where the covered  
18 entity has "actual knowledge that the information to identify an individual who is a  
subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. §  
19 164.514(b)(2)(i)(O).

20 194. Consequently, by disclosing IP addresses, Defendant's business practices violated  
21 HIPAA and industry privacy standards.

**I. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures**

195. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was marketing and profits.

196. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook and likely others in the form of enhanced advertising services and more cost-efficient marketing on its platform.

197. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

198. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

**J. Plaintiff's and Class Members' Private Information Had Financial Value**

199. The data concerning Plaintiff and Class Members, collected and shared by Defendant, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."<sup>106</sup> Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain

---

<sup>106</sup> Audience Ad Targeting, Meta, <https://www.facebook.com/business/ads/ad-targeting> (last visited Aug. 14, 2023).

1 online content.<sup>107</sup> Facebook’s “Lookalike Audiences” go further, targeting individuals who  
2 resemble current customer profiles and whom, according to Facebook, “are likely to be interested  
3 in your business.”<sup>108</sup>

4 200. Data harvesting is big business, and it drives Facebook’s profit center, its  
5 advertising sales. In 2019, Facebook generated nearly \$70 billion dollars in advertising revenue  
6 alone, constituting more than 98% of its total revenue for that year.<sup>109</sup>

7 201. This business model is not limited to Facebook. Data harvesting one of the fastest  
8 growing industries in the country, and consumer data is so valuable that it has been described as  
9 the “new oil.” Conservative estimates suggest that in 2018, Internet companies earned \$202 per  
10 American user from mining and selling data. That figure is only due to keep increasing; estimates  
11 for 2022 were as high as \$434 per user, for a total of more than \$200 billion industry wide.

12 202. In particular, the value of health data is well-known due to the media’s extensive  
13 reporting on the subject. For example, Time Magazine published an article in 2017 titled “How  
14 Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry.” Therein, Time Magazine  
15 described the extensive market for health data and observed that the health data market is both  
16 lucrative and a significant risk to privacy.<sup>110</sup>

17 203. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-  
18 identified patient data has become its own small economy: There’s a whole market of brokers who  
19

---

20 <sup>107</sup> *Id.*

21 <sup>108</sup> See How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center,  
<https://www.facebook.com/business/help/465262276878947> (last visited Aug. 14, 2023).

22 <sup>109</sup> See Here’s How Big Facebook’s Ad Business Really Is, CNN,  
<https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html> (last visited  
23 Aug. 14, 2023).

<sup>110</sup> See Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry,  
TIME, (Jan. 9, 2017 at 9:00 a.m.) <https://time.com/4588104/medical-data-industry/>.

1 compile the data from providers and other health-care organizations and sell it to buyers.”<sup>111</sup>

2 **TOLLING, CONCEALMENT, AND ESTOPPEL**

3 204. The applicable statutes of limitation have been tolled as a result of Banner’s  
4 knowing and active concealment and denial of the facts alleged herein.

5 205. Banner seamlessly incorporated Meta Pixel and other trackers into its Website and  
6 Online Platforms while providing users with no indication that their Website usage was being  
7 tracked and transmitted to third parties. Banner knew that its Website incorporated Meta Pixel and  
8 other trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical  
9 information would be intercepted, collected, used by, and disclosed to Facebook and likely other  
10 third parties.

11 206. Plaintiff and Class Members could not with due diligence have discovered the full  
12 scope of Banner’s conduct, because there were no disclosures or other indication that they were  
13 interacting with websites employing Meta Pixel or any other tracking technology.

14 207. All applicable statutes of limitation have also been tolled by operation of the  
15 discovery rule and the doctrine of continuing tort. Banner’s illegal interception and disclosure of  
16 Plaintiff’s Private Information has continued unabated. What is more, Banner was under a duty to  
17 disclose the nature and significance of its data collection practices but did not do so. Banner is  
18 therefore estopped from relying on any statute of limitations defenses.

19  
20  
21  
22  
23 <sup>111</sup> See Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html>.

1 **CLASS ALLEGATIONS**

2 208. Plaintiff brings this nationwide class action individually, and on behalf of all other  
3 similarly situated persons, pursuant to Cal. Civ. P. § 382.

4 209. The nationwide Class that Plaintiff seeks to represent is defined as follows:

5 **All persons whose Private Information was disclosed by Defendant to third**  
6 **parties through the Meta Pixel and related technology without authorization.**

7 210. Excluded from the Class are the following individuals and/or entities: Defendant  
8 and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which  
9 Defendant has a controlling interest; all individuals who make a timely election to be excluded  
10 from this proceeding using the correct protocol for opting out; any and all federal, state, or local  
11 governments, including but not limited to their departments, agencies, divisions, bureaus, boards,  
12 sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this  
13 litigation, as well as their immediate family members.

14 211. Plaintiff reserves the right to modify or amend the definition of the proposed class  
15 before the Court determines whether certification is appropriate.

16 212. Numerosity: Class Members are so numerous that joinder of all members is  
17 impracticable. Upon information and belief, there are hundreds or thousands of individuals whose  
18 Private Information may have been improperly used or disclosed by Defendant, and the Class is  
19 identifiable within Defendant's records.

20 213. Commonality: Questions of law and fact common to the Class exist and  
21 predominate over any questions affecting only individual Class Members. These include:

- 22 a. whether and to what extent Defendant had a duty to protect Plaintiff's and  
23 Class Members' Private Information;
- b. whether Defendant had duties not to disclose the Plaintiff's and Class

- 1 Members' Private Information to unauthorized third parties;
- 2 c. whether Defendant had duties not to use Plaintiff's and Class Members'
- 3 Private Information for non-healthcare purposes;
- 4 d. whether Defendant had duties not to use Plaintiff's and Class Members'
- 5 Private Information for unauthorized purposes;
- 6 e. whether Defendant failed to adequately Plaintiff's and Class Members'
- 7 Private Information;
- 8 f. whether Defendant adequately, promptly, and accurately informed Plaintiff
- 9 and Class Members that their Private Information had been compromised;
- 10 g. whether Defendant violated the law by failing to promptly notify Plaintiff
- 11 and Class Members that their Private Information had been compromised;
- 12 h. whether Defendant failed to properly implement and configure the tracking
- 13 software on its Online Platforms to prevent the disclosure of confidential
- 14 communications and Private Information;
- 15 i. whether Defendant committed invasion of privacy;
- 16 j. whether Defendant breached its implied contracts with Plaintiff and the
- 17 Class Members;
- 18 k. or in the alternate, whether Defendant was unjustly enriched;
- 19 l. whether Defendant breached fiduciary duties to Plaintiff and the Class
- 20 Members;
- 21 m. whether Defendant violated the California Invasion of Privacy Act
- 22 ("CIPA"), Cal. Penal Code §§ 630, *et seq.*;
- 23 n. whether Defendant violated the California Confidentiality of Medical



Information Act (“CMIA”), Cal. Civil Code §§ 56.06, 56.10, and 56.101;

o. whether Defendant violated the Comprehensive Computer Data Access and

Fraud Act (“CDAFA”), Cal. Penal Code § 502;

p. whether Defendant engaged in unfair, unlawful, or deceptive practices in violation of Cal. Bus. & Prof. Code §§ 17200, *et. seq.*; and,

q. whether Plaintiff and the Class Members are entitled to monetary damages, including compensatory and statutory damages, and the sums thereof.

214. Typicality: Plaintiff’s claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant’s use and incorporation of Meta Pixel and other tracking technology.

215. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court’s imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant’s policies challenged herein apply to and affect Class Members uniformly, and Plaintiff’s challenge of these policies hinges on Defendant’s conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

216. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

1           217. Superiority and Manageability: Class litigation is an appropriate method for fair  
2 and efficient adjudication of the claims involved. Class action treatment is superior to all other  
3 available methods for the fair and efficient adjudication of the controversy alleged herein; it will  
4 permit a large number of Class Members to prosecute their common claims in a single forum  
5 simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and  
6 expense that hundreds of individual actions would require. Class action treatment will permit the  
7 adjudication of relatively modest claims by certain Class Members, who could not individually  
8 afford to litigate a complex claim against large corporations, like Defendant. Further, even for  
9 those Class Members who could afford to litigate such a claim, it would still be economically  
10 impractical and impose a burden on the courts.

11           218. The nature of this action and the nature of laws available to Plaintiff and Class  
12 Members make the use of the class action device a particularly efficient and appropriate procedure  
13 to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device  
14 were not used, Defendant would necessarily gain an unconscionable advantage because they would  
15 be able to exploit and overwhelm the limited resources of each individual Class Member with  
16 superior financial and legal resources. Moreover, the costs of individual suits could unreasonably  
17 consume the amounts that would be recovered, whereas proof of a common course of conduct to  
18 which Plaintiff were exposed is representative of that experienced by the Class and will establish  
19 the right of each Class Member to recover on the cause of action alleged. Finally, individual actions  
20 would create a risk of inconsistent results and would be unnecessary and duplicative of this  
21 litigation.

22           219. The litigation of the claims brought herein is manageable. Defendant's uniform  
23 conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

1 Members demonstrates that there would be no significant manageability problems with  
2 prosecuting this lawsuit as a class action.

3 220. Adequate notice can be given to Class Members directly using information  
4 maintained in Defendant's records.

5 221. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful  
6 use and disclosure and failure to properly secure the Private Information of Class Members,  
7 Defendant may continue to refuse to provide proper notification to and obtain proper consent from  
8 Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

9 222. Further, Defendant has acted or refused to act on grounds generally applicable to  
10 the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the  
11 whole of the Class is appropriate.

12 223. Likewise, particular issues are appropriate for certification because such claims  
13 present only particular, common issues, the resolution of which would advance the disposition of  
14 this matter and the parties' interests therein. Such particular issues include, but are not limited to  
15 the following:

- 16 a. whether Defendant owed a legal duty to Plaintiff and Class Members to  
17 exercise due care in collecting, storing, using, and safeguarding their Private  
18 Information;
- 19 b. whether Defendant breached a legal duty to Plaintiff and Class Members to  
20 exercise due care in collecting, storing, using, and safeguarding their Private  
21 Information;
- 22 c. whether Defendant failed to comply with its own policies and applicable  
23 laws, regulations, and industry standards relating to the disclosure of patient

1 information;

2 d. whether an implied contract existed between Defendant on the one hand,  
3 and Plaintiff and Class Members on the other, and the terms of that implied  
4 contract;

5 e. whether Defendant breached the implied contract;

6 f. in the alternate, whether Defendant was unjustly enriched;

7 g. whether Defendant adequately and accurately informed Plaintiff and Class  
8 Members that their Private Information had been used and disclosed to third  
9 parties;

10 h. whether Defendant failed to implement and maintain reasonable security  
11 procedures and practices;

12 i. whether Defendant committed an invasion of privacy;

13 j. whether Defendant had fiduciary duties to Plaintiff and the Class Members;

14 k. whether Defendant breached its fiduciary duties;

15 l. whether Defendant violated the California Invasion of Privacy Act  
16 (“CIPA”), Cal. Penal Code §§ 630, *et seq.*;

17 m. whether Defendant violated the California Confidentiality of Medical  
18 Information Act (“CMIA”), Cal. Civil Code §§ 56.06, 56.10, and 56.101;

19 n. whether Defendant violated the Comprehensive Computer Data Access and  
20 Fraud Act (“CDAFA”), Cal. Penal Code § 502;

21 o. whether Defendant engaged in unfair, unlawful, or deceptive practices in  
22 violation of Cal. Bus. & Prof. Code §§ 17200, *et. seq.*; and,

23 p. whether Plaintiff and the Class Members are entitled to actual,

1 consequential, and/or nominal damages, and/or injunctive relief as a result  
2 of Defendant's wrongful conduct.

3 **COUNT I**  
4 **NEGLIGENCE**  
**(On Behalf of Plaintiff and the Class)**

5 224. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

6 225. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care  
7 in handling and using Plaintiff's and Class Members' Private Information in its care and custody,  
8 including implementing industry-standard privacy procedures sufficient to reasonably protect the  
9 information from the disclosure and unauthorized transmittal and use of Private Information that  
10 occurred.

11 226. Defendant acted with wanton and reckless disregard for the privacy and  
12 confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing  
13 access to this information to third parties for the financial benefit of the third parties and Defendant.

14 227. Defendant owed these duties to Plaintiff and Class Members because they are  
15 members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew  
16 or should have known would suffer injury-in-fact from Defendant's Disclosure of their Private  
17 Information to benefit third parties and Defendant. Defendant actively sought and obtained  
18 Plaintiff's and Class Members' Private Information.

19 228. Private Information is highly valuable, and Defendant knew, or should have known,  
20 the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private  
21 Information to third parties. This disclosure was of benefit to third parties and Defendant by way  
22 of data harvesting, advertising, and increased sales.

23 229. Defendant breached its common law duties by failing to exercise reasonable care

1 in the handling and securing of Private Information of Plaintiff and Class Members and in the  
2 supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private  
3 Information of Plaintiff and Class Members. This failure actually and proximately caused  
4 Plaintiff's and Class Members' injuries.

5 230. In addition, the standards of care owed by Defendant are established by statute,  
6 including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160  
7 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health  
8 Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected  
9 Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections  
10 identified above, under which Defendant were required by law to maintain adequate and  
11 reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and  
12 Class Members' Private Information.

13 231. Plaintiff and Class Members are within the class of persons that these statutes and  
14 rules were designed to protect.

15 232. Defendant had a duty to have procedures in place to detect and prevent the loss or  
16 unauthorized dissemination of Plaintiff's and Class Members' Private Information, PII and PHI.

17 233. Defendant owed a duty to timely and adequately inform Plaintiff and Class  
18 Members, in the event of their Private Information, PII and PHI, being improperly disclosed to  
19 unauthorized third parties.

20 234. It was not only reasonably foreseeable, but it was intended, that the failure to  
21 reasonably protect and secure Plaintiff's and Class Members' Private Information, PII and PHI, in  
22 compliance with applicable laws would result in an unauthorized third-parties such as Facebook,  
23 and others gaining access to Plaintiff's and Class Members' PII and PHI, and resulting in

1 Defendant's liability under principles of negligence and negligence *per se*.

2 235. Defendant violated the standards of care under Section 5 of the FTC Act and under  
3 HIPAA and attendant regulations by failing to use reasonable measures to protect Plaintiff's and  
4 Class Members' PII and PHI and not complying with applicable industry standards as described  
5 in detail herein.

6 236. As a direct and traceable result of Defendant's negligence and/or negligent  
7 supervision, and/or negligence *per se*, Plaintiff and Class Members have suffered or will suffer  
8 damages, including monetary damages, inappropriate advertisements, and use of their Private  
9 Information for advertising purposes, and increased risk of future harm, embarrassment,  
10 humiliation, frustration, and emotional distress.

11 237. Plaintiff's and Class Member's PII and PHI constitute personal property that was  
12 taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury, and  
13 damages to Plaintiff and Class Members.

14 238. Defendant's breach of its common-law duties to exercise reasonable care and  
15 negligence directly and proximately caused Plaintiff's and Class Members' actual, tangible, injury-  
16 in-fact and damages, including, without limitation, the unauthorized access of their Private  
17 Information by third parties, improper disclosure of their Private Information, lost benefit of their  
18 bargain, lost value of their Private Information and diminution in value, emotional distress, and  
19 lost time and money incurred to mitigate and remediate the effects of use of their information that  
20 resulted from and were caused by Defendant's negligence. These injuries are ongoing, imminent,  
21 immediate, and continuing.

22 239. In failing to secure Plaintiff's and Class Members' Private Information, PII and  
23 PHI, Defendant are guilty of oppression, fraud, or malice. Defendant acted or failed to act with a



1 reckless, willful, or conscious disregard of Plaintiff and Class Members' rights. Plaintiff, in  
2 addition to seeking actual damages, also seek punitive damages on behalf of themselves and the  
3 Class.

4 240. Defendant's negligence directly and proximately caused the unauthorized access  
5 and Disclosure of Plaintiff's and Class Members' Private Information, PII and PHI, and as a result,  
6 Plaintiff and Class Members have suffered and will continue to suffer damages as a result of  
7 Defendant's conduct. Plaintiff and Class Members seek actual, compensatory, and punitive  
8 damages, and all other relief they may be entitled to as a proximate result of Defendant's  
9 negligence and negligence *per se*.

10 **COUNT II**  
11 **BREACH OF IMPLIED CONTRACT**  
**(On behalf of Plaintiff and the Class)**

12 241. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

13 242. As a condition of receiving medical care from Defendant, Plaintiff and the Class  
14 provided their Private Information and paid monies for medical treatment received. In so doing,  
15 Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant  
16 agreed to safeguard and protect such information, as set forth in its Privacy Policies, and elsewhere,  
17 to keep such information secure and confidential.

18 243. Implicit in the agreement between Defendant and its patients, Plaintiff and the  
19 proposed Class Members, was the obligation that all parties would maintain the Private  
20 Information confidentially and securely.

21 244. Defendant had an implied duty of good faith to ensure that the Private Information  
22 of Plaintiff and Class Members in its possession was only used only as authorized, such as to  
23 provide medical treatment, billing, and other medical benefits from Defendant.

1           245. Defendant had an implied duty to protect the Private Information of Plaintiff and  
2 Class Members from unauthorized disclosure or uses.

3           246. Additionally, Defendant explicitly promised to keep its patients' Private  
4 Information secure and confidential, stating in its Notice of Privacy Practices that, "[o]ther uses  
5 and disclosures not described in this notice will be made only with your written  
6 authorization, such as sale of medical information.." <sup>112</sup>

7           247. Plaintiff and Class Members fully performed their obligations under the implied  
8 contracts with Defendant, but Banner did not. Plaintiff and Class Members would not have  
9 provided their confidential Private Information to Defendant in the absence of their implied  
10 contracts with Defendant that their Private Information would be kept in confidence and would  
11 instead have retained the opportunity to control their Private Information for uses other than  
12 receiving medical treatment from Defendant.

13           248. Defendant breached the implied contracts with Plaintiff and Class members by  
14 disclosing Plaintiff's and Class Members' Private Information to unauthorized third parties.

15           249. Defendant's acts and omissions have materially affected the intended purpose of  
16 the implied contracts that required Plaintiff and Class Members to provide their Private  
17 Information in exchange for medical treatment and benefits.

18           250. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff  
19 and the Class have suffered (and will continue to suffer) actual, tangible, injury-in-fact and  
20 damages, including, without limitation, the unauthorized access of their Private Information by  
21 third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost  
22 value of their Private Information and diminution in value, emotional distress, and lost time and  
23

---

<sup>112</sup> *Notice of Privacy Practices, Exhibit B* (bold emphasis added).

1 money incurred to mitigate and remediate the effects of use of their information that resulted from  
2 and were caused by Defendant's breach of implied contract. These injuries are ongoing, imminent,  
3 immediate, and continuing.

4 251. As a direct and proximate result of Defendant's above-described breach of contract,  
5 Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

6 **COUNT III**  
7 **UNJUST ENRICHMENT**  
8 **(On Behalf of Plaintiff and the Class)**

8 252. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

9 253. This claim is pleaded solely in the alternative to Plaintiff's breach of implied  
10 contract claim.

11 254. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the  
12 form of valuable sensitive medical information that Defendant collected from Plaintiff and Class  
13 Members under the guise of keeping this information private. Defendant collected, used, and  
14 disclosed this information for their own gain, for marketing purposes, and for sale or trade with  
15 third parties.

16 255. Plaintiff and Class Members would not have used Defendant's services or would  
17 have paid less for those services, if they had known that Defendant would collect, use, and disclose  
18 their Private Information to third parties.

19 256. Defendant appreciated or had knowledge of the benefits conferred upon them by  
20 Plaintiff and Class Members.

21 257. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual  
22 damages in an amount equal to the difference in value between their purchases made with  
23 reasonable data privacy practices and procedures that Plaintiff and Class Members paid for, and

1 those purchases without unreasonable data privacy practices and procedures that they received.

2 258. The benefits that Defendant derived from Plaintiff and Class Members rightly  
3 belong to Plaintiff and Class Members themselves. Under unjust enrichment principles, it would  
4 be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and  
5 unconscionable methods, acts, and trade practices alleged in this Complaint.

6 259. Defendant should be compelled to disgorge into a common fund for the benefit of  
7 Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its  
8 conduct and the unauthorized Disclosure alleged herein.

9 **COUNT IV**  
10 **BREACH OF FIDUCIARY DUTY**  
**(On Behalf of Plaintiff and the Class)**

11 260. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

12 261. A relationship existed between Plaintiff and the Class, on the one hand, and  
13 Defendant, on the other, in which Plaintiff and the Class put their trust in Defendant to protect the  
14 Private Information of Plaintiff and the Class, and Defendant accepted that trust.

15 262. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class  
16 Members by failing to act with the utmost good faith, fairness, and honesty; failing to act with the  
17 highest and finest loyalty; and failing to protect and, indeed, intentionally disclosing, their Private  
18 Information.

19 263. Defendant's breach of fiduciary duty was a legal cause of injury-in-fact and  
20 damages to Plaintiff and the Class.

21 264. But for Defendant's breach of fiduciary duty, the injury-in-fact and damages to  
22 Plaintiff and the Class would not have occurred.

23 265. Defendant's breach of fiduciary duty substantially contributed to the injury and

1 damages to the Plaintiff and the Class.

2 266. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff  
3 and Class Members are entitled to and demand actual, consequential, and nominal damages,  
4 injunctive relief, and all other relief allowed by law.

5 **COUNT V**  
6 **INVASION OF PRIVACY—INTRUSION UPON SECLUSION**  
7 **(On Behalf of Plaintiff and the Class)**

8 267. Plaintiff re-allege and incorporate the above allegations as if fully set forth herein.

9 268. Plaintiff and Class Members had a reasonable expectation of privacy in their  
10 communications with Defendant via its Websites and Online Platforms.

11 269. Plaintiff and Class Members communicated sensitive PHI and PII—Private  
12 Information—that they intended for only Defendant to receive and that they understood Defendant  
13 would keep private.

14 270. Defendant's disclosure of the substance and nature of those communications to  
15 third parties without the knowledge and consent of Plaintiff and Class Members is an intentional  
16 intrusion on Plaintiff's and Class Members' solitude or seclusion in their private affairs and  
17 concerns.

18 271. Plaintiff and Class Members had a reasonable expectation of privacy given  
19 Defendant's representations in its Privacy Policies, and elsewhere. Moreover, Plaintiff and Class  
20 Members have a general expectation that their communications regarding healthcare with their  
21 healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is  
22 highly offensive to the reasonable person.

23 272. As a result of Defendant's tortious conduct, Plaintiff and Class Members have  
suffered harm and injury, including but not limited to an invasion of their privacy rights.

273. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

274. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to, damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

275. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

276. Plaintiff also seek such other relief as the Court may deem just and proper.

**COUNT VI**  
**INVASION OF PRIVACY**  
**CAL. CONST. ART. 1 § 1**  
**(On Behalf of Plaintiff and the Class)**

277. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

278. California established the right to privacy in Article I, Section I of the California Constitution.

279. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Websites and Online Platforms.

280. Plaintiff and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Defendant to receive and that they understood Defendant would keep private.

281. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional

1 intrusion on Plaintiff's and Class Members' solitude or seclusion in their private affairs and  
2 concerns.

3 282. Plaintiff and Class Members had a reasonable expectation of privacy given  
4 Defendant's representations in their Privacy Policies, and elsewhere. Moreover, Plaintiff and Class  
5 Members have a general expectation that their communications regarding healthcare with their  
6 healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is  
7 highly offensive to the reasonable person.

8 283. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm  
9 and injury, including but not limited to an invasion of their privacy rights under the California  
10 Constitution.

11 284. Plaintiff and Class Members have been damaged as a direct and proximate result  
12 of Defendant's invasion of their privacy and are entitled to just compensation, including monetary  
13 damages.

14 285. Plaintiff and Class Members seek appropriate relief for that injury, including but  
15 not limited to, damages that will reasonably compensate Plaintiff and Class Members for the harm  
16 to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

17 286. Plaintiff and Class Members are also entitled to punitive damages resulting from  
18 the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff  
19 and Class Members in conscious disregard of their rights. Such damages are needed to deter  
20 Defendant from engaging in such conduct in the future.

21 287. Plaintiff also seek such other relief as the Court may deem just and proper.  
22  
23



**COUNT VII**  
**VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (“CIPA”),**  
**CAL. PENAL CODE §§ 630, *ET SEQ.***  
**(On Behalf of Plaintiff and the Class)**

288. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

289. The California Legislature enacted the California Invasion of Privacy Act, Cal.

Penal Code §§ 630, *et seq.* (“CIPA”) declaring that:

...advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

The Legislature by this chapter intends to protect the right of privacy of the people of this state.

Cal. Penal Code §§ 630.

290. Cal. Penal Code § 631(a) prohibits persons from “aid[ing], agree[ing] with, employ[ing], or conspir[ing] with” a third party to “read[], or attempt[] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained” “by means of any machine, instrument, or contrivance, or in any other manner...” Cal. Penal Code § 631(a).

291. Cal. Penal Code § 632(a) prohibits persons from intentionally recording confidential communications without consent of all parties to the communication.

292. All alleged communications between Plaintiff or Class Members and Defendant qualify as protected communications under CIPA because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive

1 communications in whole or in part through the use of facilities used for the transmission of  
2 communications aided by wire, cable, or other like connections.

3 293. As alleged in the preceding paragraphs, by use of the Meta Pixel and other tracking  
4 technologies, Defendant used a recording device to record the confidential communications  
5 without the consent of Plaintiff or Class members and then transmitted such information to others,  
6 such as Facebook.

7 294. At all relevant times, Defendant's aiding of Facebook, and other third parties to  
8 learn the contents of communications and Defendant's recording of confidential communications  
9 was without Plaintiff's and the Class Members' authorization and consent.

10 295. Plaintiff and Class Members had a reasonable expectation of privacy regarding the  
11 confidentiality of their communications with Defendant. Defendant promised them that it would  
12 safeguard their personal information, and that "[o]ther uses and disclosures not described in this  
13 notice will be made only with your written authorization, such as sale of medical information..."<sup>113</sup>  
14 Defendant never received any authorization and disclosed Plaintiff's and the Class's Private  
15 Information anyways.

16 296. Defendant engaged in and continued to engage in interception by aiding others  
17 (including Facebook) to secretly record the contents of Plaintiff's and Class Members' wire  
18 communications.

19 297. The intercepting devices used in this case include, but are not limited to:

- 20 a. those to which Plaintiff's and Class Members' communications were  
21 disclosed;  
22 b. Plaintiff's and Class Members' personal computing devices;  
23

---

<sup>113</sup> *Notice of Privacy Practices, Exhibit B.*

- c. Plaintiff's and Class Members' web browsers;
- d. Plaintiff's and Class Members' browser-managed files;
- e. the Meta Pixel;
- f. internet cookies;
- g. other pixels, trackers, and/or tracking technology installed on Defendant's Website and/or server;
- h. Defendant's computer servers;
- i. third-party source code utilized by Defendant; and
- j. computer servers of third parties (including Facebook).

298. Defendant aided in the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the third parties, including Facebook, include information which identifies the parties to each communication, their existence, and their contents.

299. Plaintiff and Class Members reasonably expected that their Private Information was not being intercepted, recorded, and disclosed to Facebook, and other third parties.

300. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information to Facebook, and other third parties. Neither Plaintiff nor Class Members consented to the disclosure of their Private Information by Defendant to Facebook, and other third parties.

301. The tracking pixels that Defendant utilized are designed such that they transmitted each of a website user's actions to third parties alongside and contemporaneously with the user initiating the communication. Thus, Plaintiff and Class Members' communications were intercepted in transit to the intended recipient (Defendant) before they reached Defendant's

1 servers.

2 302. Defendant willingly facilitated Facebook's interception and collection of Plaintiff's  
3 and Class Members' Private Information by embedding pixels on its Online Platforms. Moreover,  
4 Defendant had full control over these tracking pixels, including which webpages contained the  
5 pixels, what information was tracked and shared, and how events were categorized prior to  
6 transmission.

7 303. Defendant gave substantial assistance to Facebook in violating the privacy rights  
8 of its patients, despite the fact that Defendant's conduct constituted a breach of the duties of  
9 confidentiality that medical providers owe their patients. Defendant knew that the installation of  
10 the Meta Pixel on its website would result in the unauthorized disclosure of its patients'  
11 communications to Facebook, yet nevertheless did so anyway.

12 304. Plaintiff's and Class Members' electronic communications were intercepted during  
13 transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their  
14 Private Information, including using their sensitive medical information to develop marketing and  
15 advertising strategies. The private information that Defendant assisted Facebook, and other third  
16 parties with reading, learning, and exploiting, including Plaintiff's and Class Member's medical  
17 conditions, their medical concerns, and their past, present, and future medical treatment.

18 305. Plaintiff and the Class Members seek statutory damages under Cal. Penal Code §  
19 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount  
20 of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as  
21 injunctive or other equitable relief.

22 306. In addition to statutory damages, Defendant's violations caused Plaintiff and Class  
23 Members the following damages.

- a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private.
- b. Defendant eroded the essential confidential nature of the doctor-patient relationship.
- c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value;
- d. Plaintiff and Class Members did not get the full value of the medical services for which they paid, which included Defendant's duty to maintain confidentiality; and
- e. Defendant's actions diminished the value of Plaintiff's and Class Members' personal information.

307. Plaintiff and Class Members also seek such other relief as the Court may deem equitable, legal, and proper.

**COUNT VIII**  
**VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL  
INFORMATION ACT ("CMIA"), CAL. CIVIL CODE §§ 56.06, 56.10, 56.101**  
**(On behalf of Plaintiff and the Class)**

308. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

**Civil Code § 56.06**

309. Defendant is a provider of health care under Cal. Civil Code. § 56.06, subdivisions (a) and (b), because it maintains medical information and offers software to consumers that is designed to maintain medical information for the purposes of allowing their users to manage their information or for the diagnosis, treatment, or management of a medical condition.

1           310. Defendant is therefore subject to the requirements of the CMIA and obligated under  
2 Cal. Civil Code. § 56.06(d) to maintain the same standards of confidentiality required of a provider  
3 of health care with respect to medical information disclosed to it.

4           311. By conduct complained of in the preceding paragraphs, Defendant violated Cal.  
5 Civil Code § 56.06 by failing to maintain the confidentiality of users' medical information, Private  
6 Information, and instead, disclosing Plaintiff's and Class Members' medical information/Private  
7 Information to Facebook and likely other third parties without consent. This information was  
8 intentionally shared with Facebook and others, whose business is to sell advertisements based on  
9 the data that they collect about individuals, including the data Plaintiff and the Class Members  
10 shared with Defendant.

11           312. As set forth above, Defendant knowingly shared information such as identities,  
12 device identifiers, IP addresses, web URLs, possibly Facebook IDs, and other data that could be  
13 used to identify Plaintiff and Class Members in combination with their health information, such as  
14 searches and appointments. This information constitutes confidential information under the CMIA.

15           313. Defendant knowingly and willfully, or negligently, disclosed medical information  
16 of Plaintiff and the proposed Class, without consent, to Facebook for financial gain. Defendant's  
17 acts were knowing and willful as Defendant were aware that Facebook would collect all data  
18 inputted while using their websites, yet intentionally embedded Meta Pixel anyway.

19           314. Defendant's decisions to affirmatively share and communicate its patients'  
20 PHI/Private Information with Facebook resulted in one or more unauthorized persons improperly  
21 accessing and reviewing Plaintiff's and the Class Members' PHI.  
22  
23

1 Cal. Civil Code § 56.10(a)

2 315. Cal. Civil Code § 56.10(a) prohibits a health care provider from disclosing medical  
3 information without first obtaining an authorization, unless a statutory exception applies.

4 316. By conduct complained of in the preceding paragraphs, Defendant disclosed  
5 medical information, Private Information, of Plaintiff and the Class Members without first  
6 obtaining authorization when it disclosed their sensitive medical information to Facebook, and  
7 other third parties without consent, including PHI and PII. No statutory exception applies.

8 317. As a result, Defendant violated Cal. Civil Code § 56.10(a).

9 Cal. Civil Code § 56.101(a)

10 318. Cal. Civil Code § 56.101(a) requires that every provider of health care “who  
11 creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall  
12 do so in a manner that preserves the confidentiality of the information contained therein.”

13 319. Any health care provider who “negligently creates, maintains, preservers, stores,  
14 abandons, destroys, or disposes of medical information shall be subject to the remedies and  
15 penalties provided under subdivisions (b) and (c) of Section 56.36.”

16 320. By conduct complained of in the preceding paragraphs, Defendant failed to  
17 maintain, preserve, and store medical information/Private Information of Plaintiff and the Class  
18 Members in a manner that preserves the confidentiality of the information contained therein by  
19 disclosing their PHI/Private Information to Facebook, and other third parties without consent.

20 321. Defendant’s failures to maintain, preserve, and store medical information in a  
21 manner that preserves the confidentiality of the information was, at the least, negligent and violates  
22 Cal. Civil Code § 56.36(b) and (c).

1           322. Accordingly, as a result of Defendant's violations of Cal. Civil Code §§ 56.06,  
2 56.10, and Cal. Civil Code 56.101, Plaintiff and Class Members are entitled to: (1) nominal  
3 damages of \$1,000; (2) actual damages, in an amount to be determined at trial; (3) statutory  
4 damages pursuant to 56.36(c); and (4) reasonable attorney's fees and other litigation costs  
5 reasonably incurred.

6           323. In addition to statutory damages, Defendant's breach of Cal. Civil Code §§ 56.06,  
7 56.10, and 56.101, caused Plaintiff and Class Members, at minimum, the following damages:

- 8           a. Sensitive and confidential information that Plaintiff and Class Members  
9 intended to remain private is no longer private.
- 10           b. Defendant eroded the essential confidential nature of the doctor-patient  
11 relationship.
- 12           c. Defendant took something of value from Plaintiff and Class Members and  
13 derived benefit therefrom without Plaintiff's and Class Members'  
14 knowledge or informed consent and without sharing the benefit of such  
15 value;
- 16           d. Plaintiff and Class Members did not get the full value of the medical  
17 services for which they paid, which included Defendant's duty to maintain  
18 confidentiality; and
- 19           e. Defendant's actions diminished the value of Plaintiff's and Class Members'  
20 personal information.

21           324. Plaintiff and Class Members also seek such other relief as the Court may deem  
22 equitable, legal, and proper.  
23



**COUNT IX**  
**VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS**  
**AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE § 502.**  
**(On Behalf of Plaintiff and the Class)**

325. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

326. The California Legislature enacted the Comprehensive Computer Data Access and Fraud Act, CAL. PENAL CODE § 502 ("CDAFA") to "expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems," and finding and declaring "that the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data." Cal. Penal Code § 502(a).

327. In enacting the CDAFA, the Legislature further found and declared "that protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to the well-being of financial institutions, business concerns, governmental agencies, and others within this state that lawfully utilize those computers, computer systems, and data." Cal. Penal Code § 502(a).

328. Plaintiff's and the Class Members' devices on which they accessed Defendant's Online Platforms and Websites, including their computers, smart phones, and tablets, constitute computers or "computer systems" within the meaning of CDAFA. Cal. Penal Code § 502(b)(5).

329. By conduct complained of in the preceding paragraphs, Defendant violated Section 502(c)(1)(B) of CDAFA by knowingly accessing without permission Plaintiff's and Class Members' devices in order to wrongfully obtain and use their personal data, including their sensitive medical information, all Private Information, in violation of Plaintiff's and Class Members' reasonable expectations of privacy in their devices and data.

1           330. Defendant violated Cal. Penal Code § 502(c)(2) by knowingly and without  
2 permission accessing, taking, copying, and using Plaintiff's and the Class Members' Private  
3 Information, PHI and PII, including their sensitive medical information.

4           331. Defendant used Plaintiff's and Class Members' data as part of a scheme to defraud  
5 them and wrongfully obtain their data and other economic benefits. Specifically, Defendant  
6 intentionally concealed from Plaintiff and Class Members that Defendant had secretly installed  
7 tracking pixels on its Online Platforms that surreptitiously shared patient data with third party  
8 advertising companies like Facebook. Had Plaintiff and Class Members been aware of this  
9 practice, they would not have used Defendant's Website and Online Platforms.

10           332. The computers and mobile devices that Plaintiff and Class Members used when  
11 accessing Defendant's Online Platforms all have and operate "computer services" within the  
12 meaning of CDAFA. Defendant violated §§ 502(c)(3) and (7) of CDAFA by knowingly and  
13 without permission accessing and using those devices and computer services, and/or causing them  
14 to be accessed and used, *inter alia*, in connection with Facebook's wrongful collection of such  
15 data.

16           333. Under § 502(b)(12) of the CDAFA a "Computer contaminant" is defined as "any  
17 set of computer instructions that are designed to . . . record, or transmit information within a  
18 computer, computer system, or computer network without the intent or permission of the owner  
19 of the information."

20           334. Defendant violated § 502(c)(8) by knowingly and without permission introducing  
21 a computer contaminant via Meta Pixel embedded into the Online Platforms which intercepted  
22 Plaintiff's and the Class Members' private and sensitive medical information.

23           335. Defendant's violation of the CDAFA caused Plaintiff and Class Members, at

1 minimum, the following damages:

- 2 a. Sensitive and confidential information that Plaintiff and Class Members  
3 intended to remain private is no longer private.
- 4 b. Defendant eroded the essential confidential nature of the doctor-patient  
5 relationship.
- 6 c. Defendant took something of value from Plaintiff and Class Members and  
7 derived benefit therefrom without Plaintiff's and Class Members'  
8 knowledge or informed consent and without sharing the benefit of such  
9 value;
- 10 d. Plaintiff and Class Members did not get the full value of the medical  
11 services for which they paid, which included Defendant's duty to maintain  
12 confidentiality; and
- 13 e. Defendant's actions diminished the value of Plaintiff's and Class Members'  
14 Private Information.

15 336. Plaintiff and the Class Members seek compensatory damages in accordance with  
16 Cal. Penal Code § 502(e)(1), in an amount to be proved at trial, and injunctive or other equitable  
17 relief; as well as punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) as  
18 Defendant's violations were willful and, upon information and belief, Defendant is guilty of  
19 oppression, fraud, or malice as defined in Cal. Civil Code § 3294; and reasonable attorney's fees  
20 under § 502(e)(2).

21 337. Plaintiff and Class Members also seek such other relief as the Court may deem  
22 equitable, legal, and proper.  
23

**COUNT X**  
**VIOLATION OF CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.***  
**(On Behalf of Plaintiff and the Class)**

338. Plaintiff re-allege and incorporate the above allegations as if fully set forth herein.

339. Plaintiff, and Defendant are each a “person” under Cal. Bus. & Prof. Code § 17201.

340. The California Business and Professions Code §§ 17201, *et seq.* prohibits acts of unfair competition, which includes unlawful business practices.

341. Defendant’s business acts and practices are “unlawful” under the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200 *et. seq.* (the “UCL”) because, as alleged above, Defendant violated California common law, and other statutes and causes of action alleged herein.

342. Defendant engaged in unlawful acts and practices by imbedding the Pixel on its Websites, which tracks, records, and transmits Plaintiff’s and Class Members’ PHI/Private Information they disclose to Defendant in confidence via the Online Platforms and Website to third parties without Plaintiff’s and Class Members’ knowledge and/or consent, in violation of the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code §§ 630, *et seq.*; the California Confidentiality of Medical Information Act (“CMIA”), CAL. CIVIL CODE §§ 56.06, 56.10, 56.101; the Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal. Penal Code § 502; and by representing that its services have characteristics, uses, or benefits that they do not have in violation of Civil Code § 1770.

343. When using Defendant’s Website and services, Plaintiff and Class Members relied on Defendant’s status as healthcare providers.

344. Inconsistent with its roles as a healthcare provider, Defendant disclosed Plaintiff’s and Class Members’ PHI/Private Information to third parties without their consent and for marketing purposes. Thus, Defendant represented that its services have characteristics, uses, or

1 benefits that they do not have and represented that its services are of a particular standard, quality,  
2 or grade when they were not, in violation of Cal. Civil Code § 1770.

3 345. Plaintiff and Class Members were reasonable to assume, and did assume, that  
4 Defendant would take appropriate measures to keep their PHI/Private Information secure and not  
5 share it with third parties without their express consent. Defendant also had a duty to disclose that  
6 they was sharing its patients' Personal Health Information with third parties. However, Defendant  
7 did not disclose at any time that they were sharing this PHI/Private Information with third parties  
8 via the Meta Pixel and other tracking technologies.

9 346. Had Plaintiff and Class Members known that Defendant would intercept, collect,  
10 and transmit their PHI/Private Information to Facebook and other third parties, Plaintiff and the  
11 Class Members would not have used Defendant's services.

12 347. Plaintiff and Class Members have a property interest in their PHI/Private  
13 Information. By surreptitiously collecting and otherwise misusing Plaintiff's and Class Members'  
14 PHI/Private Information, Defendant has taken property from Plaintiff and Class Members without  
15 providing just (or indeed any) compensation.

16 348. By deceptively collecting, using, and sharing Plaintiff's and Class Members'  
17 PHI/Private Information with Facebook and other third parties, Defendant have taken money or  
18 property from Plaintiff and Class Members. Accordingly, Plaintiff seek restitution on behalf of  
19 themselves and the Class.

20 349. Defendant's business acts and practices also meet the unfairness prong of  
21 California's Unfair Competition Law ("UCL") according to all three theories of unfairness.

22 350. First, Defendant's business acts and practices are "unfair" under the UCL pursuant  
23 to the three-part test articulated in *Camacho v. Automobile Club of Southern California* (2006) 142

1 Cal. App. 4th 1394, 1403: (a) Plaintiff and Class Members suffered substantial injury due to  
2 Defendant's Disclosure of their PHI/Private Information; (b) Defendant's disclosure of Plaintiff's  
3 and Class Members' PHI/Private Information provides no benefit to consumers, let alone any  
4 countervailing benefit that could justify Defendant's Disclosure of PHI/Private Information  
5 without consent for marketing purposes or other pecuniary gain; and (c) Plaintiff and Class  
6 Members could not have readily avoided this injury because they had no way of knowing that  
7 Defendant was implementing the Meta Pixel.

8 351. Second, Defendant's business acts and practices are "unfair" under the UCL  
9 because they are "immoral, unethical, oppressive, unscrupulous, or substantially injurious" to  
10 Plaintiff and Class Members, and "the utility of [Defendant's] conduct," if any, does not "outweigh  
11 the gravity of the harm" to Plaintiff and Class Members. *Drum v. San Fernando Valley Bar Ass'n*,  
12 (2010) 182 Cal. App. 4th 247, 257. Defendant secretly collected, disclosed, and otherwise misused  
13 Plaintiff's and Class Members' PHI/Private Information by bartering it to Facebook and other third  
14 parties in return for access to the Pixel tool. This surreptitious, willful, and undisclosed conduct is  
15 immoral, unethical, oppressive, unscrupulous, and substantially injurious. Moreover, no benefit  
16 inheres in this conduct, the gravity of which is significant.

17 352. Third, Defendant's business acts and practices are "unfair" under the UCL because  
18 they run afoul of "specific constitutional, statutory, or regulatory provisions." *Drum*, 182 Cal. App.  
19 4th at 256 (internal quotation marks and citations omitted). California has a strong public policy  
20 of protecting consumers' privacy interests, including consumers' and patients' personal data, as  
21 codified in California's Constitution in Article I, section 1; the California Invasion of Privacy Act  
22 ("CIPA"), Cal. Penal Code §§ 630, *et seq.*; the California Confidentiality of Medical Information  
23 Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, 56.101; the Comprehensive Computer Data

1 Access and Fraud Act (“CDAFA”), Cal. Penal Code § 502, among other statutes.

2 353. Defendant violated this public policy by, among other things, surreptitiously  
3 collecting, disclosing, and otherwise exploiting Plaintiff and Class Members’ PHI/Private  
4 Information by sharing that information with Facebook and other third parties via the Tracking  
5 Pixel without Plaintiff’s and/or Class Members’ consent.

6 354. Had Plaintiff and Class Members known Defendant would intercept, collect, and  
7 transmit their PHI/Private Information to Facebook and other third parties, Plaintiff and Class  
8 Members would not have used Defendant’s services.

9 355. Plaintiff and Class Members were reasonable to assume, and did assume, that  
10 Defendant would take appropriate measures to keep their PHI/Private Information secure and not  
11 share it with third parties without their express consent. Defendant was in sole possession of and  
12 had a duty to disclose the material information that Patient Plaintiff’s and Class Members’ Personal  
13 Health Information would be shared with third parties via the Meta Pixel. Defendant did not  
14 disclose at any time that they were sharing this PHI/Private Information with third parties via the  
15 Tracking Pixel.

16 356. Plaintiff and Class Members have a property interest in their PHI/Private  
17 Information. By surreptitiously collecting and otherwise misusing Plaintiff’s and Class Members’  
18 Personal Health Information, Defendant has taken property from Plaintiff and Class Members  
19 without providing just (or indeed any) compensation.

20 357. Plaintiff and Class Members have lost money and property due to Defendant’s  
21 conduct in violation of the UCL. PHI/Private Information such as that which Defendant collected  
22 and transmitted to third parties has objective monetary value. Companies are willing to pay for  
23 PHI, like the information Defendant unlawfully collected and transmitted to third parties, such as

1 Facebook. For example, Pfizer annually pays approximately \$12 million to purchase health data  
2 from various sources.<sup>114</sup>

3 358. Consumers also value their personal health data. According to the annual Financial  
4 Trust Index Survey conducted by the University of Chicago's Booth School of Business and  
5 Northwestern University's Kellogg School of Management, which interviewed more than 1,000  
6 Americans, 93 percent of survey participants would not share their health data with a digital  
7 platform for free. Half of the survey participants would only share their data for \$100,000 or more,  
8 and 22 percent would only share their data if they received between \$1,000 and \$100,000.<sup>115</sup>

9 359. By deceptively collecting, using, and sharing Plaintiff's and Class Members'  
10 PHI/Private Information with Facebook and other third parties, Defendant has taken money and/or  
11 property from Plaintiff and Class Members. Accordingly, Plaintiff seek restitution on behalf of  
12 himself and the Class.

13 360. As a direct and proximate result of Defendant's unfair and unlawful methods and  
14 practices of competition, Plaintiff and Class Members suffered actual damages, including, but not  
15 limited to, the loss of the value of their Private Health Information.

16 361. As a direct and proximate result of its unfair and unlawful business practices,  
17 Defendant has been unjustly enriched and should be required to make restitution to Plaintiff and  
18 Class Members pursuant to §§ 17203 and 17204 of the California Business & Professions Code,  
19 disgorgement of all profits accruing to Defendant because of its unlawful and unfair business  
20 practices, declaratory relief, attorney fees and costs (pursuant to Cal. Code Civ. Proc. §1021.5),  
21 and injunctive or other equitable relief.

22  
23 <sup>114</sup> <https://www.scientificamerican.com/article/how-data-brokers-make-money-off-your-medical-records/>

<sup>115</sup> <https://www.beckershospitalreview.com/healthcare-information-technology/how-much-should-health-data-cost-100k-or-more-according-to-patients.html>



**PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiff, JOHN DOE, Individually, and on behalf of all others similarly situated, prays for judgment as follows:

- A. for an Order certifying this action as a Class action and appointing Plaintiff as Class Representatives and Plaintiff's counsel as Class Counsel;
- B. for an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;
- C. for an award of punitive damages, as allowable by law;
- D. for equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;
- E. for equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity the type of Private Information compromised and unlawfully disclosed to third parties;
- F. for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;
- G. an order that Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;
- H. for an award of attorneys' fees under the common fund doctrine, and any other applicable law;
- I. costs and any other expenses, including expert witness fees incurred by Plaintiff

1 in connection with this action;

2 J. pre- and post-judgment interest on any amounts awarded; and


3 K. such other and further relief as this court may deem just and proper.

4 **DEMAND FOR JURY TRIAL**

5 Plaintiff, by counsel, hereby demands a trial by jury on all issues so triable.

6 Dated: March 14, 2024

Respectfully submitted,

7 

8  
9 Vess A. Miller (278020)  
Natalie A. Lyons (293026)  
**COHEN & MALAD, LLP**  
One Indiana Square, Suite 1400  
Indianapolis, Indiana 46204  
10 (317) 636-6481  
11 nlyons@cohenandmalad.com  
12 vmiller@cohenandmalad.com

13 Lynn A. Toops (*Pro Hac Vice* forthcoming)  
Mary Kate Dugan (*Pro Hac Vice* forthcoming)  
14 **COHEN & MALAD, LLP**  
One Indiana Square, Suite 1400  
15 Indianapolis, Indiana 46204  
(317) 636-6481  
16 ltoops@cohenandmalad.com  
mdugan@cohenandmalad.com

17  
18 J. Gerard Stranch, IV (*Pro Hac Vice* forthcoming)  
Andrew E. Mize (*Pro Hac Vice* forthcoming)  
**STRANCH, JENNINGS & GARVEY, PLLC**  
The Freedom Center  
223 Rosa L. Parks Avenue, Suite 200  
19 Nashville, Tennessee 37203  
20 (615) 254-8801  
gstranch@stranchlaw.com  
21 amize@stranchlaw.com

22  
23 Andrew Gunem (354042)  
**TURKE & STRAUSS, LLP**  
613 Williamson St., Suite 201

Madison, Wisconsin 53703  
(608) 237-1775  
[andrewg@turkestrauss.com](mailto:andrewg@turkestrauss.com)

*Counsel for Plaintiff and the Proposed Class*

Exhibit A



July 20, 2023

[Company]  
[Address]  
[City, State, Zip Code]  
Attn: [Name of Recipient]

Re: Use of Online Tracking Technologies

Dear [Name of Recipient],

The Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and the Federal Trade Commission (FTC) are writing to draw your attention to serious privacy and security risks related to the use of online tracking technologies that may be present on your website or mobile application (app) and impermissibly disclosing consumers' sensitive personal health information to third parties.

Recent research,<sup>1</sup> news reports,<sup>2</sup> FTC enforcement actions,<sup>3</sup> and an OCR bulletin<sup>4</sup> have highlighted risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies

---

<sup>1</sup> See, e.g., Mingjia Huo, Maxwell Bland, and Kirill Levchenko, *All Eyes on Me: Inside Third Party Trackers' Exfiltration of PHI from Healthcare Providers' Online Systems*, Proceedings of the 21st Workshop on Privacy in the Electronic Society (Nov. 7, 2022), <https://dl.acm.org/doi/10.1145/3559613.3563190>.

<sup>2</sup> See, e.g., Todd Feathers, Katie Palmer, and Simon Fondrie-Teitler, *Out of Control: Dozens of Telehealth Startups Sent Sensitive Health Information to Big Tech Companies*, THE MARKUP (Dec. 13, 2022), <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>.

<sup>3</sup> *U.S. v. Easy Healthcare Corp.*, Case No. 1:23-cv-3107 (N.D. Ill. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v>; *In the Matter of BetterHelp, Inc.*, FTC Dkt. No. C-4796 (July 14, 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter>; *U.S. v. GoodRx Holdings, Inc.*, Case No. 23-cv-460 (N.D. Cal. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc>; *In the Matter of Flo Health Inc.*, FTC Dkt. No. C-4747 (June 22, 2021), <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3133-flo-health-inc>.

<sup>4</sup> U.S. Dept. of Health and Human Svcs. Office for Civil Rights, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html>.

gather identifiable information about users as they interact with a website or mobile app, often in ways which are not avoidable by and largely unknown to users.

Impermissible disclosures of an individual's personal health information to third parties may result in a wide range of harms to an individual or others. Such disclosures can reveal sensitive information including health conditions, diagnoses, medications, medical treatments, frequency of visits to health care professionals, where an individual seeks medical treatment, and more. In addition, impermissible disclosures of personal health information may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others.

### **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**

If you are a covered entity or business associate ("regulated entities") under HIPAA, you must comply with the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules), with regard to protected health information (PHI) that is transmitted or maintained in electronic or any other form or medium.

The HIPAA Rules apply when the information that a regulated entity collects through tracking technologies or discloses to third parties (*e.g.*, tracking technology vendors) includes PHI. HIPAA regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to third parties or any other violations of the HIPAA Rules. OCR's December 2022 bulletin about the use of online tracking technologies by HIPAA regulated entities provides a general overview of how the HIPAA Rules apply.<sup>5</sup> This bulletin discusses what tracking technologies are and reminds regulated entities of their obligations to comply with the HIPAA Rules when using tracking technologies.

### **FTC Act and FTC Health Breach Notification Rule**

Even if you are not covered by HIPAA, you still have an obligation to protect against impermissible disclosures of personal health information under the FTC Act and the FTC Health Breach Notification Rule. This is true even if you relied upon a third party to develop your website or mobile app and even if you do not use the information obtained through use of a tracking technology for any marketing purposes. As recent FTC enforcement actions demonstrate, it is essential to monitor data flows of health information to third parties via technologies you have integrated into your website or app.<sup>6</sup> The disclosure of such information without a consumer's authorization can, in some circumstances, violate the FTC Act as well as constitute a breach of security under the FTC's Health Breach Notification Rule.<sup>7</sup> Within the last

---

<sup>5</sup> *Id.*

<sup>6</sup> See *supra* note 3.

<sup>7</sup> See Federal Trade Comm'n, *Statement of the Commission on Breaches by Health Apps and Other Connected Devices* (Sept. 15, 2021), [https://www.ftc.gov/system/files/documents/public\\_statements/1596364/statement\\_of\\_the\\_commission\\_on\\_breaches\\_by\\_health\\_apps\\_and\\_other\\_connected\\_devices.pdf](https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf).

few months, the FTC has issued a series of guidance pieces addressed to entities collecting, using, or disclosing sensitive health information.<sup>8</sup>

OCR and the FTC remain committed to ensuring that consumers' health privacy remains protected with respect to this critical issue. Both agencies are closely watching developments in this area. To the extent you are using the tracking technologies described in this letter on your website or app, we strongly encourage you to review the laws cited in this letter and take actions to protect the privacy and security of individuals' health information.<sup>9</sup>

Sincerely,

/s/

Melanie Fontes Rainer  
Director  
Office for Civil Rights  
U.S. Department of Health and Human Services

/s/

Samuel Levine  
Director  
Bureau of Consumer Protection  
Federal Trade Commission

---

<sup>8</sup> See, e.g., FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking* (Mar. 16, 2023), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>; Lesley Fair, *First FTC Health Breach Notification Rule case addresses GoodRx's not-so-good privacy practices* (Feb. 1, 2023), <https://www.ftc.gov/business-guidance/blog/2023/02/first-ftc-health-breach-notification-rule-case-addresses-goodrxs-not-so-good-privacy-practices>; Federal Trade Comm'n and the U.S. Department of Health & Human Services' Office of the National Coordinator for Health Information Technology (ONC), Office for Civil Rights (OCR), and Food and Drug Administration (FDA), *Mobile Health App Interactive Tool* (Dec. 2022), <https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool>; Kristin Cohen, *Location, health, and other sensitive information: FTC Committed to fully enforcing the law against illegal use and sharing of highly sensitive data* (July 11, 2022), <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal>.

<sup>9</sup> In addition to the HIPAA Rules, the FTC Act, and the FTC Health Breach Notification Rule, you may also be subject to other state or federal statutes that prohibit the disclosure of personal health information.

# Notice of Privacy Practices

This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully. Effective date September 23, 2013.

## Introduction

Banner is committed to protecting the confidentiality of information about you and is required by law to do so. This notice describes how we may use information about you within Banner Health and how we may disclose it to others outside Banner. We will notify you if there is a breach of your unsecured protected health information. This notice also describes the rights you have concerning your own health information.

## How will we use and disclose information about you?

**Treatment:** Banner may use information about you to provide you with medical services and supplies. We may also disclose information about you to others that need the information to treat you, such as doctors, physician assistants, nurses, medical and nursing students, technicians, therapists, emergency service and medical transportation providers, medical equipment providers, and others involved in your care. For example, we will allow your physician to have access to your medical record to assist in your treatment and for follow-up care. We may make your medical information available electronically through an electronic health information exchange to other health care providers and health plans that request your information for their treatment and payment purposes.

We may also use and disclose information about you to contact you to remind you of an upcoming appointment, to inform you about possible treatment options or alternatives, or to tell you about health-related services available to you.

**Facility Directory:** Unless you object, Banner will include your name, location in our facility, your general condition (e.g., fair, stable, critical), and your religious affiliation in our facility directory. All of this information, except religious affiliation, will be disclosed to people that ask for you by name. Information in the facility directory may be shared with clergy.

**Family Members and Others Involved in Your Care:** Banner may disclose information about you to a family member or friend who is involved in your medical care. If you do not want the facility to disclose information about you to family members or others, you must notify the registration and nursing staff at the facility. In the event of a disaster, we may disclose information about you to help locate a family member or friend.

**Payment:** Banner may use and disclose information about you to get paid for the medical services and supplies we provide to you. For example, your health plan or health insurance company may request to see parts of your medical record before they will pay us for your treatment.

**Health Care Operations:** Banner may use and disclose information about you if it is necessary to improve the quality of care we provide to patients or for health care operations. We may use information about you to conduct quality improvement activities, to obtain audit, accounting, or legal services, or to conduct business management and planning. For example, we may use medical information to review our treatment and services and to evaluate the performance of our staff in caring for you.

**Fundraising:** Many of our patients like to make contributions to support the care provided by Banner Health. Banner or its institutionally related foundations may contact you in the future to raise funds for this purpose. You will be provided the option of not receiving these communications. Your medical information is not shared for the purpose of fundraising.

**Research:** Banner may use or disclose information about you for research projects, such as studying the effectiveness of a treatment you received. These research projects must go through a special process that protects the confidentiality of your information.

**Required by Law:** Federal, state, or local laws do not require patient consent to disclose information that is required to be reported. For instance, we are required to report child abuse and neglect, gunshot wounds, etc. Public policy has determined that these types of needs outweigh the patient's right to privacy. Banner is also required to give information to the state workers' compensation program for work-related injuries.

**Public Health:** Banner may report certain medical information for public health purposes. For instance, we are required by law to report births, deaths, and communicable diseases to the state. We may also need to report patient problems with medications or medical products to the manufacturer and to the FDA.

**Public Safety:** Banner may disclose medical information for public safety purposes in limited circumstances. We may disclose medical information to law enforcement officials or to the court in response to a search warrant or other court order. We may also disclose medical information to assist law enforcement officials in identifying or locating a person, to prosecute a crime of violence, or to report deaths that may have resulted from criminal conduct at the facility. We may also disclose information about you to law enforcement officials and others to prevent a serious threat to health or safety.

**Health Oversight Activities:** Banner may disclose medical information to a government or oversight agency that oversees Banner facilities or its personnel, such as the state's department of health services, or other federal agencies that oversee Medicare, or licensing agencies that govern physicians and other health care professionals.

**Coroners, Medical Examiners, and Funeral Directors:** Banner may disclose medical information concerning deceased patients to coroners, medical examiners, and funeral directors to assist them in carrying out their duties.

**Organ and Tissue Donation:** Banner may disclose medical information to organizations that handle organ or tissue donation or transplantation.

**Military Veterans, National Security, and Other Government Purposes:** If you are a member of the armed forces, we may release information about you as required by military command authorities or to the Department of Veterans Affairs. We may also disclose medical information to federal or state officials for intelligence and national security purposes.

**Judicial Proceedings:** Banner may disclose medical information in a lawsuit where your health status is an issue. For example, Banner may be ordered to do so by court order or search warrant.



## Notice of Privacy Practices

**Information with Additional Protection:** Certain types of medical information may have additional protection under state or federal law. For instance, medical information about communicable disease, HIV/AIDS, drug and alcohol abuse treatment, psychotherapy notes, genetic testing, or a court-ordered mental evaluation. Banner may obtain your authorization to release this information except as required by law.

**Other Uses and Disclosures:** Other uses and disclosures not described in this notice will be made only with your written authorization, such as sale of medical information. You may revoke such an authorization by sending us a written request.

### What are your rights?

**Right to Request Information About You:** You or your legally authorized representative are entitled to online access of documents available, review or receive paper copies, or request an electronic delivery of your health information. This includes your medical and billing information. If you request a copy of your information, we may charge you for our costs. We will tell you in advance what this cost will be.

**Right to Request to Amend or Supplement Information About You That You Believe is Incorrect or Incomplete:** If you see information about you and believe that some of the information is incorrect or incomplete, you may ask us to amend your record. You may submit a request to amend your medical information by contacting Health Information Management Services or the Business Office for your billing information.

**Right to Get a List of Certain Disclosures of Information About You:** You have the right to request a list of certain disclosures we made of information about you. If you would like to receive such a list, contact Health Information Management Services. We will provide the first list to you at no charge, but we may charge you for any additional lists you request during a twelve-month period. We will tell you in advance what this list will cost.

**Right to Request Restrictions on How Banner Health Will Use or Disclose Information About You for Treatment, Payment, or Health Care Operations:** You have the right to request us not to use or disclose information about you to treat you, to seek payment for care, or to operate the health care system. We are not required to agree to your request, but if we do agree, we will comply with that agreement unless that information is necessary to provide you emergency treatment. You may request that we withhold information from your health plan for the purpose of payment or health care operations, provided it is not otherwise required by law. If you want to request a restriction to your medical information, you may contact Health Information Management Services, or for billing information, you may contact the Business Office.

You have the right to pay for an item or service and elect not to have this information about you submitted to your health insurance plan. We are not required to accept your request until you have paid for this service or item. We are not required to notify other health care providers of these types of restrictions: this is your responsibility.

**Right to Request Confidential Communications:** You have the right to request us to communicate with you in a way that you feel is more confidential. You can ask to speak with your health care providers in private, outside the presence of other patients. We will accommodate reasonable requests, including alternative addresses or alternative

means. For example, you can ask us not to call your home, but to communicate only by mail. To do this, submit your request in writing to Health Information Management Services.

**Right to a Copy of Banner Health's Notice of Privacy Practices:** You have the right to a paper copy of the notice at any time. You may obtain a copy of the notice from our web site at [www.BannerHealth.com](http://www.BannerHealth.com), or you may obtain a paper copy of the notice at patient registration sites.

### Changes to this notice

We may amend or revise our practices concerning how we will use or disclose patient medical information, or how we will implement patient rights concerning their information. We reserve the right to change this notice and to make the provisions in our new notice effective for all your information. If we change these practices, we will publish a revised Notice of Privacy Practices.

### Which health care providers does this notice cover?

This Notice of Privacy Practices applies to Banner facilities and its personnel, volunteers, students, and trainees. The notice also applies to other health care providers that come to the facility to care for patients, such as physicians, physician assistants, therapists, emergency services providers, medical transportation companies, medical equipment suppliers, and other health care providers not employed by Banner unless these health care providers give you their own Notice of Privacy Practices. Banner may share your medical information with other health care providers for their treatment, payment, and health care operations.

### Do you have concerns or complaints?

Please tell us about any problems or concerns you have with your privacy rights or how Banner uses or discloses information about you. If you have a concern, you may contact Patient Relations/Administration by calling our main switchboard at 602-747-4000, and they will direct your call to the appropriate facility. You may also file a complaint with the U. S. Department of Health & Human Services, Office for Civil Rights.

We will not penalize you or take any retaliatory action against you in any way for filing a complaint with the federal government.

### Do you have questions?

Banner Health is required by law to give you this notice and to follow terms of the notice that is currently in effect. If you have any questions about this notice, or have further questions about how we may use and disclose information about you, please contact Patient Relations/Administration.



# Banner Health Privacy Statement

[Back To Legal Notices](#)

## Privacy



*Last Updated: November 2019*

This Privacy Statement describes and applies to the information we collect from you when you use voice, mobile device and desktop Banner Health platforms, tools and applications, BannerHealth.com and other Banner Health websites (collectively the "Services"), how we use that information, and when we disclose it. It will also give you more information about how to manage the personal information that you provide to us through the Services. This statement applies only to information you provide to us online while visiting or using our Services. It does not apply to information we have obtained or may obtain offline through other traditional means.

This Privacy Statement does not apply to any third-party applications that integrate with the Services.

Banner Health also maintains a separate Terms of Use that applies to your use of the Services and a Notice of Privacy Practices, as required by law, that applies to protected health information that it collects from individuals. [View our statement in English or Spanish.](#)

## 1. The information we collect.

When you use our Services, we receive and collect certain information. The information that we receive and collect depends on what you do when you use the Services.

### **Automatically Collected Information.**

Some information is automatically received and sometimes collected from you when you use the Services. This information may include some or all of the following items: the name of the domain and host from which you access the Internet, including the Internet protocol (IP) address of the computer you are using and the IP address of your Internet Service Provider; the type and version of Internet browser software you use and your operating system; the type and version of your media player(s); the date and time you access our Services, the length of your stay and the specific pages, images, video or forms that you access while using the Services; the Internet address of the website from which you linked directly to our Services and, if applicable, the search engine that referred you and any search strings or phrases that you entered into the search engine to find the Services; and demographic information concerning the country of origin of your computer and the language(s) used by it. We use this information to monitor the usage of our Services, assess performance, ensure technological compatibility with your computer, and understand the relative importance of the information provided on our Services. We may also use this data to conduct statistical analyses on visitors' usage patterns and other aggregated data.

Feedback

### **Information Collected via Cookies.**

"Cookies" are small files or records that we place on your computer's hard drive to distinguish you from other visitors using the Services. The use of cookies is a standard practice among websites to collect or track information about your activities while using the Services. Some websites use persistent cookies, which are placed on your computer and remain there until you delete them. Others use temporary cookies, which expire after some period or become overwritten by other data. Banner Health Services use "session cookies" which disappear from your computer after you have closed your Internet browser.

Most people do not know that cookies are being placed on their computers when they use Banner Health Services or most other websites because browsers are typically set to accept cookies. You can choose to have your browser warn you every time a cookie is being sent to you or you can turn off cookie placements. If you refuse cookies, you can still use Banner Health Services, but your overall experience may be affected and some functionality may be reduced or unavailable.

**Information Collected Using Pixel Tags or Clear GIFs.**

Pixel Tags or Clear GIFs, also known as Web Beacons or Web Bugs, are transparent graphical images placed on a website. Currently, Banner Health does not use them on its site.

**Information You Actively Submit.**

For most of the activity using our Services, we neither require nor collect "User Information." User Information is information that could personally identify you, for example, your name, e-mail address, billing address, shipping address(es), phone number, social security number, and credit card information. You can browse Banner Health Services and take as much time as you want to review our services without having to submit such User Information.

User Information is required when you want to (i) submit a job application; (ii) make an online donation; (iii) sign up for a class or event conducted at one of our medical centers; (iv) send an e-mail message to us or otherwise provide online comments, criticisms, suggestions or feedback; (v) participate in a chat session; (vi) purchase merchandise from the Banner Store; (vii) reserve a spot or make an appointment at a Banner Health facility; or (viii) pre-register for a hospital procedure such as surgery.

Banner Health uses a third party to host the Banner Store. If you purchase merchandise from Banner Health, Banner Health will share your User Information, including, your name, address, telephone number, credit card number, and billing and shipping address, with third parties filling your order. Banner Health does not warrant and cannot guarantee the information privacy policies and practices of such third parties.

If you make donations, your information is provided to one or more of the following 501(c)(3) organizations: Banner Health Foundation; Banner Alzheimer's Foundation; Casa Grande Community Hospital Foundation; Banner Lassen Medical Center Foundation; McKee Wellness Foundation; Weld Legacy Foundation; East Morgan County Hospital Foundation; Sterling Regional MedCenter Foundation; Ogallala Community Hospital Foundation; Community Hospital Foundation; Platte County Memorial Hospital Foundation; and/or Washakie Hospital Foundation.

We do not require you to provide any personal medical information about yourself to us through the Services, and we ask that you not share personal medical information through the Services, especially information that you wish to keep confidential. Information you provide through our Services is not protected under confidentiality laws that protect physician-patient communications. Please carefully select what you choose to disclose. In addition, while Banner Health attempts to prevent unauthorized access to our Services, such access may occur. Personal medical information that Banner Health receives in any manner is subject to separate privacy practices. [Our statement regarding the treatment of such information can be read in English or Spanish.](#)

**Personal Information about Children.**

The Banner Health Services are targeted primarily for use by adults. Accordingly, we do not knowingly collect age identifying information, except on job applications and reservation forms, nor do we knowingly collect any personal information from children under the age of 13. However, we advise all visitors utilizing our Services under the age of 13 not to disclose or provide any User Information on our Services. In the event that we discover that a child under the age of 13 has provided User Information to us, in accordance with the Children's Online Privacy Protection Act (see the [Federal Trade Commission's web site](#) for more information about this Act), we will delete the child's User Information from our files to the extent technologically possible.

## 2. How we use and share User Information.

When you actively submit User Information through the Services, we will use that information in one or more of the following ways:

- To process, complete or otherwise act upon or respond to your request or reason for submitting that information;
- To register and/or verify you in connection with a service or feature that you are attempting to access or obtain;
- To communicate with you about your request or reason for submitting that information;
- To provide additional information to you about Banner Health and its services that we believe may interest you;

- To assist, when necessary, in protecting our rights or property, enforcing the provisions of our Privacy Statement and Terms of Use, and/or preventing harm to you or others.

*We do not sell User Information to third parties.* And except where we otherwise obtain your express permission, we share your User Information with third parties only under the limited circumstances stated below:

- Credit card authorization companies receive the credit card number and other personal identifying information only to verify the credit card numbers and process a transaction.
- User Information is disclosed to third parties necessary to process a particular request you have made, to complete a purchase order for merchandise and to deliver your purchase to you or to process a donation.
- User Information submitted regarding a job application may be disclosed to third parties to conduct background checks, obtain credit reports, verify prior employment, check references and for any other lawful purpose that is in our judgment reasonably necessary to our interviewing and hiring process.
- User Information is subject to disclosure in response to judicial or other governmental subpoenas, warrants and court orders served on Banner Health in accordance with their terms, or as otherwise required by applicable law.
- User Information is subject to disclosure to protect our rights or property, to enforce the provisions of our Privacy Statement and Terms of Use, and/or to prevent harm to you or others.
- User Information may be disclosed and transferred if Banner Health or its business is sold or offered for sale to another company or person(s), if a petition for relief under the United States Bankruptcy Laws is filed by or against Banner Health, or if Banner Health becomes subject to an order of appointment of a trustee or receiver.
- If you communicate with us via e-mail, we will share your correspondence, including any User Information provided in the e-mail, with employees, volunteers, representatives, or agents most capable of addressing your correspondence. We will retain your communication until we have done our very best to provide you with a complete and satisfactory response and may subsequently retain your communication for our records.

Except where we are compelled by law to disclose your User Information, you have a right to choose whether we disclose your User Information to a third party or use your User Information for a purpose incompatible with the purpose(s) for which it was originally provided or subsequently authorized by you. Except where we are compelled by law to maintain your User Information, you also have a right to choose whether we keep your User Information. Please notify us using the contact information provided below if you wish to opt out of any such use. Please be aware that opting out of certain third-party use may prevent us from providing the services or products that you request.

All comments, feedback, suggestions, ideas, and other submissions disclosed, submitted, or offered to Banner Health regarding your use of our Services (collectively "Comments") shall be and remain the property of Banner Health. Unless otherwise prohibited by law, you agree that Banner Health may use or disclose Comments in any manner, without restriction and without compensation to you.

### 3. Linking to third-party websites.

When you click on links in our Services that take you to third-party websites, you will be subject to the third parties' privacy policies. While we support the protection of privacy on the Internet, *Banner Health cannot be responsible for the actions of any third-party websites.* We encourage you to read the posted privacy statement of any and every site you visit, whether you are linking from our Services or browsing on your own.

### 4. Access to and managing your User Information.

We believe it is important for you to be able to find out what User Information you have provided to us through our Services. If you have provided us with User Information, you can contact us to request that we provide you with the User Information we have in our records about you. We reserve the right to limit the number of times such a request can be made and to charge you for responding to such requests if this process is misused or abused. You may contact us using the contact information provided below to inquire about your User Information, and to correct, amend, or delete such information. We want the User Information we have on record about you to be as complete and accurate as possible.

If you believe that any User Information we have in our records about you is inaccurate, incomplete, or incompatible with the purposes for which it was provided or subsequently authorized by you, please notify us using the contact information provided below.

## 5. What you need to do to protect your Personally Identifiable Information.

You have several options when deciding how you can best protect your User Information. One option is simply not to volunteer it. As stated above, this approach would allow you to still use our Services – although it will prevent you from taking advantage of some of our Services' features, for example, completing an order, making an appointment and signing up for classes. The Federal Trade Commission's website, [www.ftc.gov](http://www.ftc.gov), also offers useful information about how to protect User Information provided to a website.

## 6. What to do about suspected violations of this Privacy Statement.

If at any time you believe Banner Health has not adhered to the policies and principles set forth in this Privacy Statement, please notify us using the contact information provided below. We will make all commercially reasonable efforts to promptly address your concerns.

## 7. Changes to Privacy Statement.

This Privacy Statement was last modified on the date noted above. If we change our Privacy Statement, we will post those changes on our website so you are always aware of what information we collect, how we use it, how we protect it and under what circumstances, if any, we disclose it. If we make material changes, we will also post a notice on our home page, which notice will run for seven consecutive days following the effective date of the modified privacy statement. Unless we clearly express otherwise, we will use information in accordance with the Privacy Statement under which the information was collected. YOU ARE HEREBY ADVISED THAT YOUR CONTINUED USE OF OUR SERVICES CONSTITUTES YOUR ACCEPTANCE OF ANY AMENDMENTS TO AND THE MOST RECENT VERSION OF THIS PRIVACY STATEMENT.

## 8. Questions, comments and contact information.


If you have any questions or comments concerning our Privacy Statement, please contact us through our [online form](#).

The image shows a screenshot of the Banner Health website footer and a newsletter sign-up form. The form is titled "Sign up for our healthy living newsletter" and includes an "Email" input field and a "JOIN" button. Below the form is the Banner Health logo. At the bottom, there are two columns of links: "Banner Health", "Doctors", "Services", and "Locations" on the left; and "About", "Executive Leadership", "Quality", and "News" on the right.

Sign up for our healthy living newsletter

Email

JOIN

 **Banner Health.**

Banner Health

Doctors

Services

Locations

About

Executive Leadership

Quality

News

[For Health Professionals](#)

[For Media](#)

[For Employees](#)

[Ways to Give](#)

[Volunteers](#)

[Donate Now](#)

[Insurance](#)

[Careers](#)

**Patient Center**

**Connect With Us**

[Bill Pay and Information](#)

[Contact](#)

[Classes and Events](#)

[Read Our Blog](#)

[Health and Wellness](#)

[Ask an Expert](#)

[Help Paying Your Bill](#)

[Newsletter Sign Up](#)

[Medical Records](#)

[Patient Account](#)

[Patient Registration](#)

[Price Transparency](#)



[Terms of Use](#)

[Privacy Statement](#)

[Nondiscrimination](#)

© 2024 By Banner Health

# Banner Health Privacy Statement

[Back To Legal Notices](#)

## Privacy



*Last Updated: November 2019*

This Privacy Statement describes and applies to the information we collect from you when you use voice, mobile device and desktop Banner Health platforms, tools and applications, BannerHealth.com and other Banner Health websites (collectively the "Services"), how we use that information, and when we disclose it. It will also give you more information about how to manage the personal information that you provide to us through the Services. This statement applies only to information you provide to us online while visiting or using our Services. It does not apply to information we have obtained or may obtain offline through other traditional means.

This Privacy Statement does not apply to any third-party applications that integrate with the Services.

Banner Health also maintains a separate Terms of Use that applies to your use of the Services and a Notice of Privacy Practices, as required by law, that applies to protected health information that it collects from individuals. [View our statement in English or Spanish.](#)

## 1. The information we collect.

When you use our Services, we receive and collect certain information. The information that we receive and collect depends on what you do when you use the Services.

### **Automatically Collected Information.**

Some information is automatically received and sometimes collected from you when you use the Services. This information may include some or all of the following items: the name of the domain and host from which you access the Internet, including the Internet protocol (IP) address of the computer you are using and the IP address of your Internet Service Provider; the type and version of Internet browser software you use and your operating system; the type and version of your media player(s); the date and time you access our Services, the length of your stay and the specific pages, images, video or forms that you access while using the Services; the Internet address of the website from which you linked directly to our Services and, if applicable, the search engine that referred you and any search strings or phrases that you entered into the search engine to find the Services; and demographic information concerning the country of origin of your computer and the language(s) used by it. We use this information to monitor the usage of our Services, assess performance, ensure technological compatibility with your computer, and understand the relative importance of the information provided on our Services. We may also use this data to conduct statistical analyses on visitors' usage patterns and other aggregated data.

Feedback

### **Information Collected via Cookies.**

"Cookies" are small files or records that we place on your computer's hard drive to distinguish you from other visitors using the Services. The use of cookies is a standard practice among websites to collect or track information about your activities while using the Services. Some websites use persistent cookies, which are placed on your computer and remain there until you delete them. Others use temporary cookies, which expire after some period or become overwritten by other data. Banner Health Services use "session cookies" which disappear from your computer after you have closed your Internet browser.

Most people do not know that cookies are being placed on their computers when they use Banner Health Services or most other websites because browsers are typically set to accept cookies. You can choose to have your browser warn you every time a cookie is being sent to you or you can turn off cookie placements. If you refuse cookies, you can still use Banner Health Services, but your overall experience may be affected and some functionality may be reduced or unavailable.



Pixel Tags or Clear GIFs, also known as Web Beacons or Web Bugs, are transparent graphical images placed on a website. Currently, Banner Health does not use them on its site.

### Information You Actively Submit.

For most of the activity using our Services, we neither require nor collect "User Information." User Information is information that could personally identify you, for example, your name, e-mail address, billing address, shipping address(es), phone number, social security number, and credit card information. You can browse Banner Health Services and take as much time as you want to review our services without having to submit such User Information.

User Information is required when you want to (i) submit a job application; (ii) make an online donation; (iii) sign up for a class or event conducted at one of our medical centers; (iv) send an e-mail message to us or otherwise provide online comments, criticisms, suggestions or feedback; (v) participate in a chat session; (vi) purchase merchandise from the Banner Store; (vii) reserve a spot or make an appointment at a Banner Health facility; or (viii) pre-register for a hospital procedure such as surgery.

Banner Health uses a third party to host the Banner Store. If you purchase merchandise from Banner Health, Banner Health will share your User Information, including, your name, address, telephone number, credit card number, and billing and shipping address, with third parties filling your order. Banner Health does not warrant and cannot guarantee the information privacy policies and practices of such third parties.

If you make donations, your information is provided to one or more of the following 501(c)(3) organizations: Banner Health Foundation; Banner Alzheimer's Foundation; Casa Grande Community Hospital Foundation; Banner Lassen Medical Center Foundation; McKee Wellness Foundation; Weld Legacy Foundation; East Morgan County Hospital Foundation; Sterling Regional MedCenter Foundation; Ogallala Community Hospital Foundation; Community Hospital Foundation; Platte County Memorial Hospital Foundation; and/or Washakie Hospital Foundation.

We do not require you to provide any personal medical information about yourself to us through the Services, and we ask that you not share personal medical information through the Services, especially information that you wish to keep confidential. Information you provide through our Services is not protected under confidentiality laws that protect physician-patient communications. Please carefully select what you choose to disclose. In addition, while Banner Health attempts to prevent unauthorized access to our Services, such access may occur. Personal medical information that Banner Health receives in any manner is subject to separate privacy practices. [Our statement regarding the treatment of such information can be read in English or Spanish.](#)

### Personal Information about Children.

The Banner Health Services are targeted primarily for use by adults. Accordingly, we do not knowingly collect age identifying information, except on job applications and reservation forms, nor do we knowingly collect any personal information from children under the age of 13. However, we advise all visitors utilizing our Services under the age of 13 not to disclose or provide any User Information on our Services. In the event that we discover that a child under the age of 13 has provided User Information to us, in accordance with the Children's Online Privacy Protection Act (see the [Federal Trade Commission's web site](#) for more information about this Act), we will delete the child's User Information from our files to the extent technologically possible.

## 2. How we use and share User Information.

When you actively submit User Information through the Services, we will use that information in one or more of the following ways:

- To process, complete or otherwise act upon or respond to your request or reason for submitting that information;
- To register and/or verify you in connection with a service or feature that you are attempting to access or obtain;
- To communicate with you about your request or reason for submitting that information;
- To provide additional information to you about Banner Health and its services that we believe may interest you;
- To study and analyze the use of the information and features available on our Services; and

- To assist, when necessary, in protecting our rights or property, enforcing the provisions of our Privacy Statement and Terms of Use, and/or preventing harm to you or others.

*We do not sell User Information to third parties.* And except where we otherwise obtain your express permission, we share your User Information with third parties only under the limited circumstances stated below:

- Credit card authorization companies receive the credit card number and other personal identifying information only to verify the credit card numbers and process a transaction.
- User Information is disclosed to third parties necessary to process a particular request you have made, to complete a purchase order for merchandise and to deliver your purchase to you or to process a donation.
- User Information submitted regarding a job application may be disclosed to third parties to conduct background checks, obtain credit reports, verify prior employment, check references and for any other lawful purpose that is in our judgment reasonably necessary to our interviewing and hiring process.
- User Information is subject to disclosure in response to judicial or other governmental subpoenas, warrants and court orders served on Banner Health in accordance with their terms, or as otherwise required by applicable law.
- User Information is subject to disclosure to protect our rights or property, to enforce the provisions of our Privacy Statement and Terms of Use, and/or to prevent harm to you or others.
- User Information may be disclosed and transferred if Banner Health or its business is sold or offered for sale to another company or person(s), if a petition for relief under the United States Bankruptcy Laws is filed by or against Banner Health, or if Banner Health becomes subject to an order of appointment of a trustee or receiver.
- If you communicate with us via e-mail, we will share your correspondence, including any User Information provided in the e-mail, with employees, volunteers, representatives, or agents most capable of addressing your correspondence. We will retain your communication until we have done our very best to provide you with a complete and satisfactory response and may subsequently retain your communication for our records.

Except where we are compelled by law to disclose your User Information, you have a right to choose whether we disclose your User Information to a third party or use your User Information for a purpose incompatible with the purpose(s) for which it was originally provided or subsequently authorized by you. Except where we are compelled by law to maintain your User Information, you also have a right to choose whether we keep your User Information. Please notify us using the contact information provided below if you wish to opt out of any such use. Please be aware that opting out of certain third-party use may prevent us from providing the services or products that you request.

All comments, feedback, suggestions, ideas, and other submissions disclosed, submitted, or offered to Banner Health regarding your use of our Services (collectively "Comments") shall be and remain the property of Banner Health. Unless otherwise prohibited by law, you agree that Banner Health may use or disclose Comments in any manner, without restriction and without compensation to you.

### 3. Linking to third-party websites.

When you click on links in our Services that take you to third-party websites, you will be subject to the third parties' privacy policies. While we support the protection of privacy on the Internet, *Banner Health cannot be responsible for the actions of any third-party websites.* We encourage you to read the posted privacy statement of any and every site you visit, whether you are linking from our Services or browsing on your own.

### 4. Access to and managing your User Information.

We believe it is important for you to be able to find out what User Information you have provided to us through our Services. If you have provided us with User Information, you can contact us to request that we provide you with the User Information we have in our records about you. We reserve the right to limit the number of times such a request can be made and to charge you for responding to such requests if this process is misused or abused. You may contact us using the contact information provided below to inquire about your User Information, and to correct, amend, or delete such information. We want the User Information we have on record about you to be as complete and accurate as possible.

If you believe that any User Information we have in our records about you is inaccurate, incomplete, or incompatible with the purposes for which it was provided or subsequently authorized by you, please notify us using the contact information provided below.



## 5. What you need to do to protect your Personally Identifiable Information.

You have several options when deciding how you can best protect your User Information. One option is simply not to volunteer it. As stated above, this approach would allow you to still use our Services – although it will prevent you from taking advantage of some of our Services' features, for example, completing an order, making an appointment and signing up for classes. The Federal Trade Commission's website, [www.ftc.gov](http://www.ftc.gov), also offers useful information about how to protect User Information provided to a website.

## 6. What to do about suspected violations of this Privacy Statement.

If at any time you believe Banner Health has not adhered to the policies and principles set forth in this Privacy Statement, please notify us using the contact information provided below. We will make all commercially reasonable efforts to promptly address your concerns.

## 7. Changes to Privacy Statement.

This Privacy Statement was last modified on the date noted above. If we change our Privacy Statement, we will post those changes on our website so you are always aware of what information we collect, how we use it, how we protect it and under what circumstances, if any, we disclose it. If we make material changes, we will also post a notice on our home page, which notice will run for seven consecutive days following the effective date of the modified privacy statement. Unless we clearly express otherwise, we will use information in accordance with the Privacy Statement under which the information was collected. YOU ARE HEREBY ADVISED THAT YOUR CONTINUED USE OF OUR SERVICES CONSTITUTES YOUR ACCEPTANCE OF ANY AMENDMENTS TO AND THE MOST RECENT VERSION OF THIS PRIVACY STATEMENT.

## 8. Questions, comments and contact information.

If you have any questions or comments concerning our Privacy Statement, please contact us through our [online form](#).

The image shows a screenshot of the Banner Health website footer and a newsletter sign-up form. At the top, there is a dark blue banner with the text "Sign up for our healthy living newsletter" in white. Below this is a white input field labeled "Email" and a blue "JOIN" button. The footer area is white with the Banner Health logo on the left. To the right of the logo, there are two columns of links. The first column includes "Banner Health", "Doctors", "Services", and "Locations". The second column includes "About", "Executive Leadership", "Quality", and "News".

[For Health Professionals](#)[For Media](#)[For Employees](#)[Ways to Give](#)[Volunteers](#)[Donate Now](#)[Insurance](#)[Careers](#)[Patient Center](#)[Connect With Us](#)[Bill Pay and Information](#)[Contact](#)[Classes and Events](#)[Read Our Blog](#)[Health and Wellness](#)[Ask an Expert](#)[Help Paying Your Bill](#)[Newsletter Sign Up](#)[Medical Records](#)[Patient Account](#)[Patient Registration](#)[Price Transparency](#)[Terms of Use](#)[Privacy Statement](#)[Nondiscrimination](#)

© 2024 By Banner Health

# Banner Health Terms of Use

Exhibit D

[Back To Legal Notices](#)

## Terms of Use

*Last Updated: November 2019*

**Do not use this website for medical emergencies. For emergency services dial 9-1-1 or your local emergency assistance number.**

**[Learn more about our Banner Health Social Media Terms of Use Agreement. \(View the Social Media Terms of Use en Español\).](#)**

### 1. Welcome

Welcome and thank you for visiting the Banner Health website ("Website") and reviewing our Terms of Use. Banner Health makes this Website, including all information, documents, catalogs, communications, files, text, graphics, and audio/visual files (collectively, the "Materials") available for your use subject to the Terms of Use set forth in this document. It spells out what you can expect from us and what we expect from you.

### 2. Terms of use, acceptance of terms of use, and non-transferability

By accessing, using or downloading in any way, without limitation, any materials from this Website or merely browsing this Website, you agree to and are bound by these Terms of Use. Please read these Terms of Use carefully. Banner Health reserves the right to change the Terms of Use at any time, without prior notice to any Website visitor ("User"). If Banner Health makes material changes to the Terms of Use, we will post a notice on our home page for seven consecutive days following the effective date of the modified Terms of Use. You are hereby advised that your continued use of our Website constitutes your acceptance of any amendments to and the most recent version of the Terms of Use. If you breach any of the Terms of Use, your authorization to use this Website automatically terminates, and any of the Materials downloaded or printed from this Website must be immediately destroyed. A User's right to use this Website is NOT transferable.

### 3. Medical disclaimers

The content of the Banner Health Website, such as text, graphics, images, information obtained from Banner Health's licensors, and other Material contained on the Banner Health Website are for informational purposes only and are not intended in any way to substitute for professional medical advice, diagnosis, or treatment. Users are encouraged to develop a professional relationship with physicians and other medical practitioners and regularly consult with them to seek their advice. Never disregard professional medical advice or delay in seeking it because of something you have read, viewed, or heard on the Banner Health Website. Users should review any information supplied to or on this Website with their own medical professional.

Banner Health's Chats and Forums are conducted or moderated by employees of Banner Health. By providing this service, our employees are not entering into a physician-patient relationship with you. Our employees will not diagnose, treat, or prescribe for anyone using our Website. Our employees will not accept payment from you and will not bill any insurance company, government payment program or other source of health benefits for information provided on our Website.

Since no physician-patient relationship exists between you and Banner Health, please do not share personal health information that you wish to keep confidential. Information you provide is not protected under confidentiality laws that protect physician-patient communications. By posting information you may be sharing your personal information. Please

Feedback

carefully select what you choose to disclose. Additionally, while Banner Health attempts to prevent unauthorized access to our Website files, such access may occur. Our employees do not keep any records of their communications on our Website and will not have any records of any prior contacts you may have had with our Website.

This Website may contain health or medical related materials that are sexually explicit. If you find these materials offensive, you may not want to use our Website.

## 4. Intellectual property rights

### A. Copyright information and personal and non-commercial use limitation

All materials and the compilation of all content included on this Website are owned or licensed by Banner Health and protected by United States and international copyright laws. Banner Health does not claim ownership of copyrights owned by third parties.

You have been granted a license to view and use the Website Materials subject to these Terms of Use. Unless otherwise specified, the Materials on this Website are for your personal and non-commercial use. You may download and make one copy of Website Materials for your own non-commercial home use, provided that you maintain all copyright, service mark and other proprietary notices. You may not sell or modify Website Materials or reproduce, distribute, display publicly or otherwise use the Website Materials in any way for any public or commercial purpose. Permission to reprint or electronically reproduce any document or graphic, in whole or in part, for any other purpose is expressly prohibited without prior written consent from Banner Health. You may contact us at 2901 North Central Avenue, Phoenix, AZ 85012, Attn: Strategic Services, Web Project Manager or [e-mail us through this form](#). Users may not provide copyrighted or other proprietary information to Banner Health without permission from the owner of such material or rights. Users are solely responsible for obtaining such permission and for any damages resulting from unauthorized disclosures.

### B. Notice and procedure for making claims under the Digital Millennium Copyright Act notice

The Digital Millennium Copyright Act (DMCA) provides recourse to copyright owners who believe that their rights under the United States Copyright Act have been infringed by acts of third parties over the Internet. If you believe that your copyrighted work has been copied without your authorization and is available on this Website in a way that may constitute copyright infringement, you may provide notice of your claim to Banner Health's designated agent listed below. For your notice to be effective, it must include the following information: (1) a physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed; (2) identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that website; (3) identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material; (4) information reasonably sufficient to permit the service provider to contact the complaining party, such as address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted; (5) a statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and (6) a statement that the information in the notification is accurate and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

If a third party has wrongly filed a copyright infringement notice with Banner Health against you, and your access to the allegedly infringing material has been disabled, you have the right to provide Banner Health's designated agent with a counter notification. That notification must include the following information: (1) physical or electronic signature of the subscriber; (2) identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled; (3) a statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification; and (4) the subscribers name, address, telephone number and e-mail address, and a statement that the subscriber consents to the jurisdiction of the Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification or an agent of such person.

Banner Health's Designated Agent is:

Attention: VP IT Business Services  
 Digital Business Technology  
 2901 North Central Ave.  
 Phoenix, AZ 85012  
 (602) 747-4000

The Designated Agent should be contacted only if you believe that your work has been used or copied in a way that constitutes copyright infringement and such infringement is occurring on this Website. All other inquiries directed to the Designated Agent will not be answered.

## C. Trademarks

Banner Health is the owner of numerous trademarks related to its health care services. These trademarks include, but are not limited to, Banner Health System®, Banner Health, Banner and Banner logos. These trademarks and other Banner Health graphics, logos and service marks are trademarks of Banner Health and may not be used without prior written consent of Banner Health. All other trademarks, product names, and company names and logos appearing on the Banner Health Website are the property of their respective owners.

## D. Ideas and inventions

All comments, feedback, suggestions, ideas, and other submissions ("Ideas") disclosed, submitted, or offered to Banner Health in connection with your use of this Website shall be the exclusive property of Banner Health. User agrees that unless otherwise prohibited by law Banner Health may use, sell, exploit and disclose the Ideas in any manner, without compensation, attribution or notification to User.

## 5. Privacy and protection of Personal Information

Banner Health respects the privacy of visitors to our Website. Please see Banner Health's Privacy Statement relating to the collection and use of your information. User acknowledges and agrees that this Privacy Statement, including but not limited to the manner that Banner Health collects, uses and discloses User's personally identifiable information, is incorporated and made part of these Terms of Use. If User does not agree to Banner Health's Privacy Statement, then User should not use this Website or submit or post any personally identifiable information on this Website. Questions regarding privacy issues should be directed to Banner Health System Web Services.

## 6. Disclaimers and limitation of liability

User expressly agrees that use of Banner Health's Website and service is at User's sole risk. Neither Banner Health, nor its affiliates, nor any of their officers, directors, or employees, agents, third-party content providers, merchants, sponsors, licensors (collectively, "Providers"), or the like, warrant that websites affiliated with Banner Health, including but not limited to [www.BannerHealth.com](http://www.BannerHealth.com), will be uninterrupted, error-free, or free of viruses, worms, Trojan horses, keyboard loggers, harmful or malicious code, or other defects. The information, products and services published on this Website may contain inaccuracies or typographical errors. The Providers make no warranty as to the results that may be obtained from the use of Banner Health's Websites or as to the accuracy, reliability, or currency of any information, content, service, or merchandise provided through Banner Health's Websites.

This Website contains several links to other websites. These websites are not under the control of Banner Health, and the existence of a link on Banner Health's Website does not imply any endorsement of the linked websites by Banner Health or any affiliation between Banner Health and the owners of the linked websites. Banner Health makes no warranties or representations, and disclaims all liability, relating to the accuracy, content, privacy policies, products, services, legality, reliability, viewpoint, accuracy, currency, decency, or any other aspect of the linked websites. You agree that Banner Health has no responsibility to you with respect to such material. Visitors to other websites are encouraged to examine the privacy policies and/or terms of use of that website.

This Website is provided by Banner Health on an "as is" and "as available" basis. Banner Health and the providers make no

services or prices offered on or through the Website, or the information, content, materials or products, included on this Website. To the fullest extent permissible by applicable law, Banner Health and the providers disclaim the warranties and conditions, express or implied, with regard to the information, content, materials, products and services available on this Website, including but not limited to, implied warranties of merchantability and fitness for a particular purpose. You expressly agree that your use of this Website is at your sole risk.

Banner Health and the providers will not be liable for any damages of any kind arising from the use of or inability to use this Website, including direct, indirect, incidental, punitive and consequential damages. No oral advice or written information given by Banner Health or its affiliates, or any of their officers, directors, employees, agents, providers, or the like, shall create a warranty of any kind,; and User shall not rely on any such information or advice. The limitation of this paragraph shall apply notwithstanding any reliance by a User on any information obtained from the Website [www.BannerHealth.com](http://www.BannerHealth.com) or that result from mistakes, omissions, interruptions, deletion of files or e-mail, errors, defects, viruses, delays on operation or transmission, or any failure of performance, whether or not resulting from acts of God, communications failure, theft, destruction, or unauthorized access to Banner Health's records, programs, or services, and whether or not Banner Health and/or any other providers have been advised of the possibility of such damages. User hereby acknowledges this paragraph shall apply to all content, merchandise, and services available through [www.BannerHealth.com](http://www.BannerHealth.com) and all other websites affiliated with Banner Health. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, in such states liability is limited to the fullest extent permitted by the law.

If you are dissatisfied with any Banner Health Website content, your sole and exclusive remedy is to discontinue your use of this Website.

## 7. Online conduct

The User agrees to use the Banner Health Website only for lawful purposes. Unacceptable uses of the Website include: (i) engaging in any illegal activity or the planning of any illegal activity; (ii) disseminating or transmitting statements or material that, to a reasonable person, may be abusive, obscene, pornographic, defamatory, harassing, grossly offensive, vulgar, threatening or malicious; (iii) creating, disseminating or transmitting files, graphics, software or other material that actually or potentially infringes the copyright, trademark, patent, trade secret, publicity or other intellectual property rights of any person; (iv) creating a false identity or otherwise attempting to mislead any person as to the identity or origin of any communication; (v) exporting, re-exporting or permitting the downloading of any message, software or content in violation of any export or import law, regulation or restriction of the United States and its agencies or authorities, or without all required approvals, licenses or exemptions; (vi) interfering, disrupting or attempting to gain unauthorized access to other accounts on the Website or any other computer network; (vii) disseminating or transmitting viruses, worms, Trojan horses, time bombs, spyware, cancelbots or any other malicious or invasive code or program; or (viii) engaging in any other activity deemed by Banner Health to be in conflict with the spirit or intent of this Website.

## 8. Credit and credit card authorization

You may pay for your orders of merchandise or donations with major credit cards issued in the United States of America. Currently, Banner Health accepts Visa®, MasterCard®, and Discover® Card. Generally, credit cards are not charged until we either ship the item(s) to you or confirm availability (at which time you will be charged only for the goods we have actually shipped along with any appropriate taxes or shipping charges). However, Banner Health may pre-authorize your order amount with your credit card issuer at the time you place the order, which may affect your available credit line. Please contact your credit card issuer for more information.

After you place an order on the Banner Health Website, we will check the information you provide for validity, by verifying your method of payment or shipping address. Banner Health reserves the right to reject any order you place with us, and/or to limit quantities on any order, without giving any reason. If we reject your order, we will attempt to notify you using the e-mail address you have given us with the order. Your credit card will normally not be charged if we reject an order, but we will process a refund if the charge has been made against your credit card.



## 9. Termination

These Terms of Use are effective until terminated by either party. You may terminate these terms at any time by discontinuing use of the Banner Health Website and destroying all Materials obtained from this Website and all copies thereof, whether made under these Terms of Use or otherwise. Your access to the Banner Health Web site may be terminated immediately without notice from Banner Health if, in our sole discretion, you fail to comply with any term or provision of these Terms of Use. Upon termination, you must cease use of the Banner Health Website and destroy all Materials obtained from this Website and all copies thereof, whether made under these Terms of Use or otherwise.

## 10. Applicable law and jurisdiction

This Website is hosted by Banner Health in the State of Arizona. As such, by visiting Banner Health's Website, even if accessed from a location outside the United States, you agree that the laws of the State of Arizona will govern these disclaimers, and Terms of Use, without giving effect to any principles of conflicts of laws. Banner Health reserves the right to make changes to its Website and these disclaimers, Terms of Use, and Privacy Statement at any time. User hereby irrevocably and unconditionally consents to jurisdiction in the State of Arizona.

## 11. Waiver and severability

The failure of Banner Health to require or enforce strict performance by User of any provision of these Terms of Use or to exercise any right under them shall not be construed as a waiver or relinquishment of Banner Health's right to assert or rely upon any such provision or right in that or any other instance.

The provisions in these Terms of Use are intended to be severable. If for any reason any provision in these Terms of Use is held invalid or unenforceable in whole or in part by any court of competent jurisdiction, such provision shall, as to such jurisdiction, be ineffective to the extent of such determination of invalidity or unenforceability without affecting the validity or enforceability thereof in any other manner and without affecting the remaining provisions hereof, which shall continue to be in full force and effect.

## 12. International Users

The Banner Health Website can be accessed from locations around the world. Banner Health makes no representations that this Website or the Materials available through it are appropriate for use in locations outside the United States. Access to this Website from locations where this Website or any of its Materials are illegal is prohibited. If you access this Website from a location outside the United States, you are responsible for compliance with all local and/or international laws.

## 13. Security

Banner Health reserves the right to monitor all network traffic to this Website to identify and/or block unauthorized attempts or intrusions to upload or change information or cause damage to this Website in any fashion. Anyone using this Website expressly consents to such monitoring.

These Terms of Use may be changed at any time, without prior notice.

Sign up for our healthy living newsletter

Email

JOIN



## Banner Health

[Doctors](#)[Services](#)[Locations](#)[For Health Professionals](#)[For Employees](#)[Volunteers](#)[Insurance](#)

## Patient Center

[Bill Pay and Information](#)[Classes and Events](#)[Health and Wellness](#)[Help Paying Your Bill](#)[Medical Records](#)[Patient Account](#)[Patient Registration](#)[Price Transparency](#)

## About

[Executive Leadership](#)[Quality](#)[News](#)[For Media](#)[Ways to Give](#)[Donate Now](#)[Careers](#)

## Connect With Us

[Contact](#)[Read Our Blog](#)[Ask an Expert](#)[Newsletter Sign Up](#)[Terms of Use](#)[Privacy Statement](#)[Nondiscrimination](#)

© 2024 By Banner Health



# Banner Health Terms of Use

Exhibit D

[Back To Legal Notices](#)

## Terms of Use



*Last Updated: November 2019*

**Do not use this website for medical emergencies. For emergency services dial 9-1-1 or your local emergency assistance number.**

**[Learn more about our Banner Health Social Media Terms of Use Agreement. \(View the Social Media Terms of Use en Español\).](#)**

### 1. Welcome

Welcome and thank you for visiting the Banner Health website ("Website") and reviewing our Terms of Use. Banner Health makes this Website, including all information, documents, catalogs, communications, files, text, graphics, and audio/visual files (collectively, the "Materials") available for your use subject to the Terms of Use set forth in this document. It spells out what you can expect from us and what we expect from you.

### 2. Terms of use, acceptance of terms of use, and non-transferability

By accessing, using or downloading in any way, without limitation, any materials from this Website or merely browsing this Website, you agree to and are bound by these Terms of Use. Please read these Terms of Use carefully. Banner Health reserves the right to change the Terms of Use at any time, without prior notice to any Website visitor ("User"). If Banner Health makes material changes to the Terms of Use, we will post a notice on our home page for seven consecutive days following the effective date of the modified Terms of Use. You are hereby advised that your continued use of our Website constitutes your acceptance of any amendments to and the most recent version of the Terms of Use. If you breach any of the Terms of Use, your authorization to use this Website automatically terminates, and any of the Materials downloaded or printed from this Website must be immediately destroyed. A User's right to use this Website is NOT transferable.

### 3. Medical disclaimers

The content of the Banner Health Website, such as text, graphics, images, information obtained from Banner Health's licensors, and other Material contained on the Banner Health Website are for informational purposes only and are not intended in any way to substitute for professional medical advice, diagnosis, or treatment. Users are encouraged to develop a professional relationship with physicians and other medical practitioners and regularly consult with them to seek their advice. Never disregard professional medical advice or delay in seeking it because of something you have read, viewed, or heard on the Banner Health Website. Users should review any information supplied to or on this Website with their own medical professional.

Banner Health's Chats and Forums are conducted or moderated by employees of Banner Health. By providing this service, our employees are not entering into a physician-patient relationship with you. Our employees will not diagnose, treat, or prescribe for anyone using our Website. Our employees will not accept payment from you and will not bill any insurance company, government payment program or other source of health benefits for information provided on our Website.

Since no physician-patient relationship exists between you and Banner Health, please do not share personal health information that you wish to keep confidential. Information you provide is not protected under confidentiality laws that protect physician-patient communications. By posting information you may be sharing your personal information. Please

Feedback

carefully select what you choose to disclose. Additionally, while Banner Health attempts to prevent unauthorized access to our Website files, such access may occur. Our employees do not keep any records of their communications on our Website and will not have any records of any prior contacts you may have had with our Website.

This Website may contain health or medical related materials that are sexually explicit. If you find these materials offensive, you may not want to use our Website.

## 4. Intellectual property rights

### A. Copyright information and personal and non-commercial use limitation

All materials and the compilation of all content included on this Website are owned or licensed by Banner Health and protected by United States and international copyright laws. Banner Health does not claim ownership of copyrights owned by third parties.

You have been granted a license to view and use the Website Materials subject to these Terms of Use. Unless otherwise specified, the Materials on this Website are for your personal and non-commercial use. You may download and make one copy of Website Materials for your own non-commercial home use, provided that you maintain all copyright, service mark and other proprietary notices. You may not sell or modify Website Materials or reproduce, distribute, display publicly or otherwise use the Website Materials in any way for any public or commercial purpose. Permission to reprint or electronically reproduce any document or graphic, in whole or in part, for any other purpose is expressly prohibited without prior written consent from Banner Health. You may contact us at 2901 North Central Avenue, Phoenix, AZ 85012, Attn: Strategic Services, Web Project Manager or [e-mail us through this form](#). Users may not provide copyrighted or other proprietary information to Banner Health without permission from the owner of such material or rights. Users are solely responsible for obtaining such permission and for any damages resulting from unauthorized disclosures.

### B. Notice and procedure for making claims under the Digital Millennium Copyright Act notice

The Digital Millennium Copyright Act (DMCA) provides recourse to copyright owners who believe that their rights under the United States Copyright Act have been infringed by acts of third parties over the Internet. If you believe that your copyrighted work has been copied without your authorization and is available on this Website in a way that may constitute copyright infringement, you may provide notice of your claim to Banner Health's designated agent listed below. For your notice to be effective, it must include the following information: (1) a physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed; (2) identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that website; (3) identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material; (4) information reasonably sufficient to permit the service provider to contact the complaining party, such as address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted; (5) a statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and (6) a statement that the information in the notification is accurate and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

If a third party has wrongly filed a copyright infringement notice with Banner Health against you, and your access to the allegedly infringing material has been disabled, you have the right to provide Banner Health's designated agent with a counter notification. That notification must include the following information: (1) physical or electronic signature of the subscriber; (2) identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled; (3) a statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification; and (4) the subscriber's name, address, telephone number and e-mail address, and a statement that the subscriber consents to the jurisdiction of the Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification or an agent of such person.

Banner Health's Designated Agent is:

Attention: VP IT Business Services  
Digital Business Technology  
2901 North Central Ave.  
Phoenix, AZ 85012  
(602) 747-4000

The Designated Agent should be contacted only if you believe that your work has been used or copied in a way that constitutes copyright infringement and such infringement is occurring on this Website. All other inquiries directed to the Designated Agent will not be answered.

## C. Trademarks

Banner Health is the owner of numerous trademarks related to its health care services. These trademarks include, but are not limited to, Banner Health System®, Banner Health, Banner and Banner logos. These trademarks and other Banner Health graphics, logos and service marks are trademarks of Banner Health and may not be used without prior written consent of Banner Health. All other trademarks, product names, and company names and logos appearing on the Banner Health Website are the property of their respective owners.

## D. Ideas and inventions

All comments, feedback, suggestions, ideas, and other submissions ("Ideas") disclosed, submitted, or offered to Banner Health in connection with your use of this Website shall be the exclusive property of Banner Health. User agrees that unless otherwise prohibited by law Banner Health may use, sell, exploit and disclose the Ideas in any manner, without compensation, attribution or notification to User.

## 5. Privacy and protection of Personal Information

Banner Health respects the privacy of visitors to our Website. Please see Banner Health's Privacy Statement relating to the collection and use of your information. User acknowledges and agrees that this Privacy Statement, including but not limited to the manner that Banner Health collects, uses and discloses User's personally identifiable information, is incorporated and made part of these Terms of Use. If User does not agree to Banner Health's Privacy Statement, then User should not use this Website or submit or post any personally identifiable information on this Website. Questions regarding privacy issues should be directed to Banner Health System Web Services.

## 6. Disclaimers and limitation of liability

User expressly agrees that use of Banner Health's Website and service is at User's sole risk. Neither Banner Health, nor its affiliates, nor any of their officers, directors, or employees, agents, third-party content providers, merchants, sponsors, licensors (collectively, "Providers"), or the like, warrant that websites affiliated with Banner Health, including but not limited to [www.BannerHealth.com](http://www.BannerHealth.com), will be uninterrupted, error-free, or free of viruses, worms, Trojan horses, keyboard loggers, harmful or malicious code, or other defects. The information, products and services published on this Website may contain inaccuracies or typographical errors. The Providers make no warranty as to the results that may be obtained from the use of Banner Health's Websites or as to the accuracy, reliability, or currency of any information, content, service, or merchandise provided through Banner Health's Websites.

This Website contains several links to other websites. These websites are not under the control of Banner Health, and the existence of a link on Banner Health's Website does not imply any endorsement of the linked websites by Banner Health or any affiliation between Banner Health and the owners of the linked websites. Banner Health makes no warranties or representations, and disclaims all liability, relating to the accuracy, content, privacy policies, products, services, legality, reliability, viewpoint, accuracy, currency, decency, or any other aspect of the linked websites. You agree that Banner Health has no responsibility to you with respect to such material. Visitors to other websites are encouraged to examine the privacy policies and/or terms of use of that website.

This Website is provided by Banner Health on an "as is" and "as available" basis. Banner Health and the providers make no representations or warranties of any kind, express or implied, as to the operation of the Website, the availability of any

services or prices offered on or through the Website, or the information, content, materials or products included on this Website. To the fullest extent permissible by applicable law, Banner Health and the providers disclaim the warranties and conditions, express or implied, with regard to the information, content, materials, products and services available on this Website, including but not limited to, implied warranties of merchantability and fitness for a particular purpose. You expressly agree that your use of this Website is at your sole risk.

Banner Health and the providers will not be liable for any damages of any kind arising from the use of or inability to use this Website, including direct, indirect, incidental, punitive and consequential damages. No oral advice or written information given by Banner Health or its affiliates, or any of their officers, directors, employees, agents, providers, or the like, shall create a warranty of any kind, and User shall not rely on any such information or advice. The limitation of this paragraph shall apply notwithstanding any reliance by a User on any information obtained from the Website [www.BannerHealth.com](http://www.BannerHealth.com) or that result from mistakes, omissions, interruptions, deletion of files or e-mail, errors, defects, viruses, delays on operation or transmission, or any failure of performance, whether or not resulting from acts of God, communications failure, theft, destruction, or unauthorized access to Banner Health's records, programs, or services, and whether or not Banner Health and/or any other providers have been advised of the possibility of such damages. User hereby acknowledges this paragraph shall apply to all content, merchandise, and services available through [www.BannerHealth.com](http://www.BannerHealth.com) and all other websites affiliated with Banner Health. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, in such states liability is limited to the fullest extent permitted by the law.

If you are dissatisfied with any Banner Health Website content, your sole and exclusive remedy is to discontinue your use of this Website.

## 7. Online conduct

The User agrees to use the Banner Health Website only for lawful purposes. Unacceptable uses of the Website include: (i) engaging in any illegal activity or the planning of any illegal activity; (ii) disseminating or transmitting statements or material that, to a reasonable person, may be abusive, obscene, pornographic, defamatory, harassing, grossly offensive, vulgar, threatening or malicious; (iii) creating, disseminating or transmitting files, graphics, software or other material that actually or potentially infringes the copyright, trademark, patent, trade secret, publicity or other intellectual property rights of any person; (iv) creating a false identity or otherwise attempting to mislead any person as to the identity or origin of any communication; (v) exporting, re-exporting or permitting the downloading of any message, software or content in violation of any export or import law, regulation or restriction of the United States and its agencies or authorities, or without all required approvals, licenses or exemptions; (vi) interfering, disrupting or attempting to gain unauthorized access to other accounts on the Website or any other computer network; (vii) disseminating or transmitting viruses, worms, Trojan horses, time bombs, spyware, cancelbots or any other malicious or invasive code or program; or (viii) engaging in any other activity deemed by Banner Health to be in conflict with the spirit or intent of this Website.

## 8. Credit and credit card authorization

You may pay for your orders of merchandise or donations with major credit cards issued in the United States of America. Currently, Banner Health accepts Visa®, MasterCard®, and Discover® Card. Generally, credit cards are not charged until we either ship the item(s) to you or confirm availability (at which time you will be charged only for the goods we have actually shipped along with any appropriate taxes or shipping charges). However, Banner Health may pre-authorize your order amount with your credit card issuer at the time you place the order, which may affect your available credit line. Please contact your credit card issuer for more information.

After you place an order on the Banner Health Website, we will check the information you provide for validity, by verifying your method of payment or shipping address. Banner Health reserves the right to reject any order you place with us, and/or to limit quantities on any order, without giving any reason. If we reject your order, we will attempt to notify you using the e-mail address you have given us with the order. Your credit card will normally not be charged if we reject an order, but we will process a refund if the charge has been made against your credit card.

## 9. Termination

These Terms of Use are effective until terminated by either party. You may terminate these terms at any time by discontinuing use of the Banner Health Website and destroying all Materials obtained from this Website and all copies thereof, whether made under these Terms of Use or otherwise. Your access to the Banner Health Web site may be terminated immediately without notice from Banner Health if, in our sole discretion, you fail to comply with any term or provision of these Terms of Use. Upon termination, you must cease use of the Banner Health Website and destroy all Materials obtained from this Website and all copies thereof, whether made under these Terms of Use or otherwise.

## 10. Applicable law and jurisdiction

This Website is hosted by Banner Health in the State of Arizona. As such, by visiting Banner Health's Website, even if accessed from a location outside the United States, you agree that the laws of the State of Arizona will govern these disclaimers, and Terms of Use, without giving effect to any principles of conflicts of laws. Banner Health reserves the right to make changes to its Website and these disclaimers, Terms of Use, and Privacy Statement at any time. User hereby irrevocably and unconditionally consents to jurisdiction in the State of Arizona.

## 11. Waiver and severability

The failure of Banner Health to require or enforce strict performance by User of any provision of these Terms of Use or to exercise any right under them shall not be construed as a waiver or relinquishment of Banner Health's right to assert or rely upon any such provision or right in that or any other instance.

The provisions in these Terms of Use are intended to be severable. If for any reason any provision in these Terms of Use is held invalid or unenforceable in whole or in part by any court of competent jurisdiction, such provision shall, as to such jurisdiction, be ineffective to the extent of such determination of invalidity or unenforceability without affecting the validity or enforceability thereof in any other manner and without affecting the remaining provisions hereof, which shall continue to be in full force and effect.

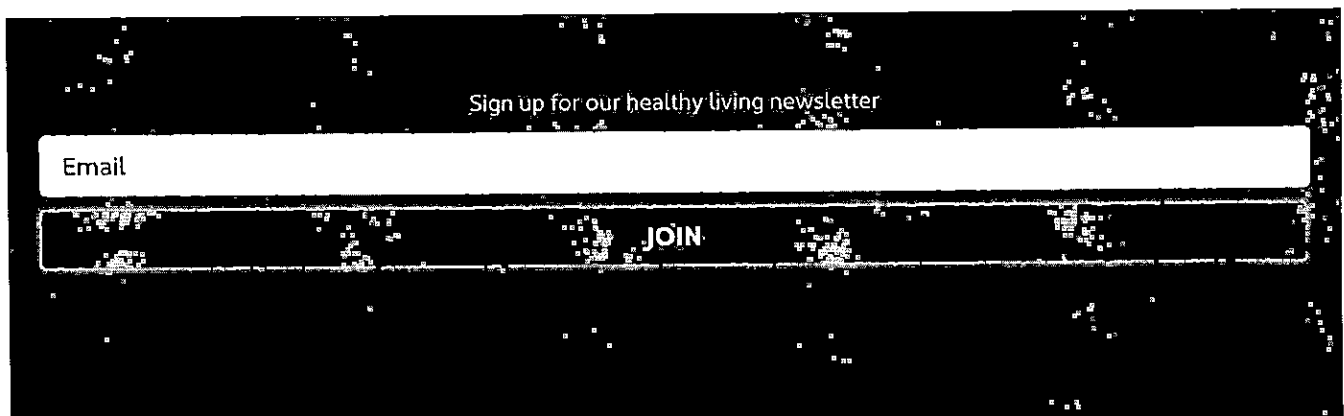
## 12. International Users

The Banner Health Website can be accessed from locations around the world. Banner Health makes no representations that this Website or the Materials available through it are appropriate for use in locations outside the United States. Access to this Website from locations where this Website or any of its Materials are illegal is prohibited. If you access this Website from a location outside the United States, you are responsible for compliance with all local and/or international laws.

## 13. Security

Banner Health reserves the right to monitor all network traffic to this Website to identify and/or block unauthorized attempts or intrusions to upload or change information or cause damage to this Website in any fashion. Anyone using this Website expressly consents to such monitoring.

These Terms of Use may be changed at any time, without prior notice.





## Banner Health.

[Doctors](#)[Services](#)[Locations](#)[For Health Professionals](#)[For Employees](#)[Volunteers](#)[Insurance](#)

## Patient Center

[Bill Pay and Information](#)[Classes and Events](#)[Health and Wellness](#)[Help Paying Your Bill](#)[Medical Records](#)[Patient Account](#)[Patient Registration](#)[Price Transparency](#)

## About

[Executive Leadership](#)[Quality](#)[News](#)[For Media](#)[Ways to Give](#)[Donate Now](#)[Careers](#)

## Connect With Us

[Contact](#)[Read Our Blog](#)[Ask an Expert](#)[Newsletter Sign Up](#)[Terms of Use](#)[Privacy Statement](#)[Nondiscrimination](#)

© 2024 By Banner Health



## **EXHIBIT 2**



CIVIL CASE

Associated Cases

Case Status

Civil Case

Civil Hearings

Judges

Judgment/Orders

ROA

CIVIL ROA SUMMARY ▶ 2024-CV0076564 JOHN DOE vs BANNER HEALTH

CASE STATUS

Advanced Search

SORT DATE

Ascending

Descending

<input type="checkbox"/>	<div><div>*DATE</div><div>04/08/2024 03:44 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Copy of Complaint sent to Pandi McVay.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>MICST</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>04/08/2024 12:00 AM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Payment received in the amount of \$57.00, receipt number CC00801.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>ACCTPMTREC</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/21/2024 04:00 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Proof of Service of Summons, Complaint, and CCCS as to BANNER HEALTH filed. Served on 03/20/2024 by Personal Service.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>DSSRV</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/15/2024 12:31 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Summons issued to BANNER HEALTH on 03/15/2024.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>DSISS</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/14/2024 03:25 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Delay Reduction Program Notice provided to DOE, JOHN.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>DELAY</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/14/2024 03:25 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Civil Case Cover Sheet filed.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>CCCS</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/14/2024 03:25 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Complaint - Unlimited Civil (over \$35,000) filed by DOE, JOHN.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>FILE</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/14/2024 03:25 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Complex Case Fee (One Fee for All Plaintiffs) filed by DOE, JOHN.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>FILE</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/14/2024 03:25 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Payment received from JOHN DOE in the amount of \$1435.00. Receipt number 37665.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>ACCTPMT</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/14/2024 03:25 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Payment received from JOHN DOE in the amount of \$1435.00. Receipt number 37665.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>ACCTPMT</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>
<input type="checkbox"/>	<div><div>*DATE</div><div>03/14/2024 03:25 PM</div></div> <div><div>SEALED</div><div><input type="checkbox"/></div></div> <div><div>*TEXT</div><div>Case initiated.</div></div>	<div><div>*JUDGE</div><div>Mallery, Tony</div></div> <div><div>CODE</div><div>CI</div></div>	<div><div>MICROFILM NUMBER</div><div></div></div> <div><div>ACTION TYPE</div><div><div></div><div></div></div></div>

LIST

REFRESH

CANCEL





**Service of Process Notification**

03/20/2024

CT Log Number 546028675

**Service of Process Transmittal Summary**

**RECEIVED**

**By Cindy Manuel at 8:44 am, Mar 22, 2024**

**TO:** Jean Lance  
Banner Health  
2901 NORTH CENTRAL AVE, SUITE 160  
PHOENIX, AZ 85012

**RE:** Process Served in California

**FOR:** Banner Health (Domestic State: CA)

**ENCLOSED ARE COPIES OF LEGAL PROCESS RECEIVED BY THE STATUTORY AGENT OF THE ABOVE COMPANY AS FOLLOWS:**

**TITLE OF ACTION:** JOHN DOE, individually and on behalf of all others similarly situated vs. BANNER HEALTH

**DOCUMENT(S) SERVED:** Summons, Class Action Complaint

**COURT/AGENCY:** Lassen County - Superior Court - Susanville, CA  
Case # 2024CV0076564

**NATURE OF ACTION:** CLASS ACTION COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF BASED UPON

**PROCESS SERVED ON:** C T Corporation System, GLENDALE, CA

**DATE/METHOD OF SERVICE:** By Process Server on 03/20/2024 at 13:28

**JURISDICTION SERVED:** California

**APPEARANCE OR ANSWER DUE:** Within 30 days after this summons

**ATTORNEY(S)/SENDER(S):** Vess A. Miller  
Cohen & Malad, LLP  
One Indiana Square, Suite 1400  
Indianapolis, IN 46204  
317-636-6481

**ACTION ITEMS:** SOP Papers with Transmittal, via UPS Next Day Air , 1ZX212780136514907  
Image SOP  
Email Notification, Banner Health Legal legaldept-serviceofprocess@bannerhealth.com  
Email Notification, Cindy Manuel cindy.manuel@bannerhealth.com  
Email Notification, Sonya Papelian sonya.papelian@bannerhealth.com

**REGISTERED AGENT CONTACT:** C T Corporation System  
330 N BRAND BLVD  
STE 700  
GLENDALE, CA 91203  
866-539-8692  
CorporationTeam@wolterskluwer.com



The information contained in this Transmittal is provided by CT for quick reference only. It does not constitute a legal opinion, and should not otherwise be relied on, as to the nature of action, the amount of damages, the answer date, or any other information contained in the included documents. The recipient(s) of this form is responsible for reviewing and interpreting the included documents and taking appropriate action, including consulting with its legal and other advisors as necessary. CT disclaims all liability for the information contained in this form, including for any omissions or inaccuracies that may be contained therein.



**PROCESS SERVER DELIVERY DETAILS**

**Date:** Wed, Mar 20, 2024  
**Server Name:** Victor Mendez

Entity Served	BANNER HEALTH
Case Number	2024CV0076564
Jurisdiction	CA

Inserts		



SUM-100

# SUMMONS (CITACION JUDICIAL)

FOR COURT USE ONLY  
(SOLO PARA USO DE LA CORTE)

**NOTICE TO DEFENDANT:**  
**(AVISO AL DEMANDADO):**  
BANNER HEALTH

**YOU ARE BEING SUED BY PLAINTIFF:**  
**(LO ESTÁ DEMANDANDO EL DEMANDANTE):**  
JOHN DOE, individually and on behalf of all others similarly situated

**NOTICE!** You have been sued. The court may decide against you without your being heard unless you respond within 30 days. Read the information below.

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the plaintiff. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center ([www.courtinfo.ca.gov/selfhelp](http://www.courtinfo.ca.gov/selfhelp)), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site ([www.lawhelpcalifornia.org](http://www.lawhelpcalifornia.org)), the California Courts Online Self-Help Center ([www.courtinfo.ca.gov/selfhelp](http://www.courtinfo.ca.gov/selfhelp)), or by contacting your local court or county bar association. **NOTE:** The court has a statutory lien for waived fees and costs on any settlement or arbitration award of \$10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case. **AVISO!** Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.

Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al demandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California ([www.sucorte.ca.gov](http://www.sucorte.ca.gov)), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.

Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services, ([www.lawhelpcalifornia.org](http://www.lawhelpcalifornia.org)), en el Centro de Ayuda de las Cortes de California, ([www.sucorte.ca.gov](http://www.sucorte.ca.gov)) o poniéndose en contacto con la corte o el colegio de abogados locales. **AVISO:** Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de \$10,000 o más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.

The name and address of the court is:  
(El nombre y dirección de la corte es): Superior Court of Lassen County, CA  
Civil Division, 2610 Riverside Drive, Susanville, CA, 96130

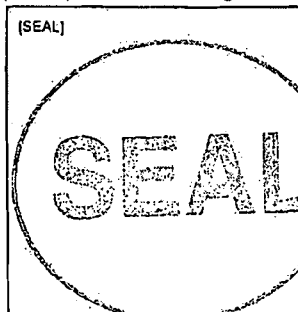
CASE NUMBER:  
(Número del Caso):

2024 CV 0076564

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is:  
(El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):  
Vess A. Miller, Cohen & Malad, LLP, One Indiana Square, Suite 1400, Indianapolis, Indiana 46204, (317) 636-6481 **T. STALTER**

DATE: **MAR 14 2024** Clerk, by **C. Crosby** Deputy  
(Fecha) (Secretario) (Adjunto)

(For proof of service of this summons, use Proof of Service of Summons (form POS-010).)  
(Para prueba de entrega de esta citación use el formulario Proof of Service of Summons, (POS-010)).



## NOTICE TO THE PERSON SERVED: You are served

1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of (specify):
3. ☒ on behalf of (specify): **Banner Health**  
under: ☒ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)  
☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)  
☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)  
☐ other (specify):
4. ☐ by personal delivery on (date):

FILE  
BY FAX

FILED  
 U.S. District Court  
 County of Lassen  
 MAR 14 2024  
 C. Crosby  
 DE: CITY CLERK

1 Andrew Gunem (354042)  
 2 TURKE & STRAUSS, LLP  
 3 613 Williamson Street, Suite 201  
 4 Madison, Wisconsin 53703  
 5 (608) 237-1775  
 6 andrewg@turkestrauss.com

Lynn A. Toops\*  
 Mary Kate Dugan\*  
 COHEN & MALAD, LLP  
 One Indiana Square, Suite 1400  
 Indianapolis, Indiana 46204  
 (317) 636-6481  
 ltoops@cohenandmalad.com  
 mdugan@cohenandmalad.com

5 Natalie A. Lyons (293026)  
 6 Vess A. Miller (278020)  
 7 COHEN & MALAD, LLP  
 8 One Indiana Square, Suite 1400  
 9 Indianapolis, Indiana 46204  
 10 (317) 636-6481  
 11 nlyons@cohenandmalad.com  
 12 vmiller@cohenandmalad.com

J. Gerard Stranch, IV\*  
 Andrew E. Mize\*  
 STRANCH, JENNINGS & GARVEY, PLLC  
 223 Rosa L. Parks Avenue, Suite 200  
 Nashville, Tennessee 37203  
 (615) 254-8801  
 jstranch@stranchlaw.com  
 amize@stranchlaw.com

10 *Counsel for Plaintiff and the Proposed Class*

\*To move for *pro hac vice* admission

11 **SUPERIOR COURT FOR THE STATE OF CALIFORNIA**  
 12 **FOR THE COUNTY OF LASSEN**

12 **JOHN DOE, individually and on behalf of**  
 13 **all others similarly situated,**

14 **Plaintiff,**

15 **v.**

16 **BANNER HEALTH**

17 **Defendant.**

Case No. 2024 CV 0 07 6 5 6 4

**CLASS ACTION COMPLAINT**  
**FOR DAMAGES AND INJUNCTIVE**  
**RELIEF BASED UPON:**

- (1) Negligence;
- (2) Breach of Implied Contract;
- (3) Unjust Enrichment;
- (4) Breach of Fiduciary Duty;
- (5) Invasion of Privacy;
- (6) Invasion of Privacy under the California Constitution, Cal. Const. Art. 1 § 1;
- (7) Violation of the California Invasion of Privacy Act, Cal. Penal Code § 630, *et seq.*
- (8) Violation of the California Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56.06, 56.10, 56.101;
- (9) Violation of the Comprehensive Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and,
- (10) Violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*

**JURY TRIAL DEMANDED**

FILE  
 BY FAX

**CLASS ACTION COMPLAINT**

Plaintiff, JOHN DOE, Individually, and on behalf of all others similarly situated (hereinafter, “Plaintiff”), brings this Class Action Complaint against Defendant, BANNER HEALTH (hereinafter, “Banner” or “Defendant”), and alleges, upon personal knowledge as to his own actions, and upon information and belief as to all other matters, as follows.

**INTRODUCTION**

1. Plaintiff brings this class action to address Defendant’s improper practice of disclosing the confidential Personally Identifying Information (“PII”)<sup>1</sup> and/or Protected Health Information (“PHI”)<sup>2</sup> (collectively referred to as “Private Information”) of Plaintiff and the proposed Class Members to third parties, including Meta Platforms, Inc. d/b/a Meta (“Facebook” or “Meta”),<sup>3</sup> Google, LLC (“Google”), Microsoft, AppDynamics, Taboola, Pinterest, StackAdapt,

---

<sup>1</sup> The Federal Trade Commission defines “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.” 17 C.F.R. § 248.201(b)(8).

<sup>2</sup> Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations (“HIPAA”), “protected health information” is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. “Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP’T FOR HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last accessed Apr. 16, 2020). Banner is clearly a “covered entity” and some of the data compromised in the Disclosure that this action arises out of is “protected health information,” subject to HIPAA.

<sup>3</sup> Facebook changed its name from Facebook, Inc. to Meta Platforms, Inc. in October 2021. Plaintiff’s reference to both “Facebook” and “Meta” throughout this complaint refer to the same company.

1 LinkedIn, Skai, Medallia, and potentially others via tracking technologies used on its website (“the  
2 Disclosure”).

3       2.       The Office for Civil Rights (“OCR”) at the U.S. Department of Health and Human  
4 Services (“HHS”) and the Federal Trade Commission (“FTC”) warn about the “serious privacy  
5 and security risks related to the use of online tracking technologies” present on websites or online  
6 platforms, such as Defendant’s, that “impermissibly disclos[e] consumers’ sensitive personal  
7 health information to third parties.”<sup>4</sup> OCR and FTC agree that such tracking technologies, like  
8 those present on Defendant’s website, “can track a user’s online activities” and “gather identifiable  
9 information about users as they interact with a website or mobile app, often in ways which are not  
10 avoidable by and largely unknown to users.”<sup>5</sup> OCR and FTC warn that “[i]mpermissible  
11 disclosures of an individual’s personal health information to third parties may result in a wide  
12 range of harms to an individual or others. Such disclosures can reveal sensitive information  
13 including health conditions, diagnoses, medications, medical treatments, frequency of visits to  
14 health care professionals, where an individual seeks medical treatment, and more. In addition,  
15 impermissible disclosures of personal health information may result in identity theft, financial loss,  
16 discrimination, stigma, mental anguish, or other serious negative consequences to the reputation,  
17 health, or physical safety of the individual or to others.”<sup>6</sup>

18       3.       Information about a person’s physical and mental health is among the most  
19 confidential and sensitive information in our society, and the mishandling of medical information  
20 can have serious consequences, including discrimination in the workplace or denial of insurance  
21

---

22 <sup>4</sup> Re: Use of Online Tracking Technologies, U.S. Dep’t of Health & Human Services (July 20,  
23 2023), available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf), **attached as Exhibit A.**

<sup>5</sup> *Id.*

<sup>6</sup> Re: Use of Online Tracking Technologies, **Exhibit A.**

1 coverage. If people do not trust that their medical information will be kept private, they may be  
2 less likely to seek medical treatment, which can lead to more serious health problems down the  
3 road. In addition, protecting medical information and making sure it is kept confidential and not  
4 disclosed to anyone other than the person's medical provider is necessary to maintain public trust  
5 in the healthcare system as a whole.

6 4. Recognizing these facts, and in order to implement requirements of the Health  
7 Insurance Portability and Accountability Act of 1996 ("HIPAA"), HHS has established "Standards  
8 for Privacy of Individually Identifiable Health Information" (also known as the "Privacy Rule")  
9 governing how health care providers must safeguard and protect Private Information. Under the  
10 HIPAA Privacy Rule, no health care provider can disclose a person's personally identifiable  
11 protected health information to a third party without express written authorization.

12 5. Headquartered in Phoenix, Arizona, Banner is a massive, national health care  
13 system treating patients in six (6) western states under a mission of "*making health care easier,*  
14 *so life can be better.*"<sup>7</sup>

15 6. Despite its unique position as a massive and trusted healthcare provider, Banner  
16 knowingly configured and implemented into its website, <https://www.bannerhealth.com/> (the  
17 "Website") code-based tracking devices known as "pixels" (also referred to as "trackers" or  
18 "tracking technologies"), which collected and transmitted patients' Private Information to  
19 Facebook and other third parties, without patients' knowledge or authorization.

20 7. Defendant encourages patients to use its Website, along with its various web-based  
21 tools and services (collectively, the "Online Platforms"), to learn about Banner on its main  
22  
23

---

<sup>7</sup> <https://www.bannerhealth.com/about> (last accessed March 8, 2024) (emphasis in original)



1 homepage,<sup>8</sup> to search for health information,<sup>9</sup> to find a doctor,<sup>10</sup> to find locations,<sup>11</sup> to learn about  
 2 medical conditions and treatment services,<sup>12</sup> to learn about classes and events,<sup>13</sup> to access a patient  
 3 portal,<sup>14</sup> to pay bills,<sup>15</sup> and more.

4 8. When Plaintiff and Class Members used Defendant's Website and Online  
 5 Platforms, they thought they were communicating exclusively with their trusted healthcare  
 6 provider. Unbeknownst to them, Defendant embedded pixels from Facebook, Google, and likely  
 7 others, into its Website and Online Platforms, surreptitiously forcing Plaintiff and Class Members  
 8 to transmit intimate details about their medical treatment to third parties without their consent.

9 9. A pixel (also referred to as a "tracker" or "tracking technology") is a snippet of  
 10 code embedded into a website that tracks information about its visitors and their website  
 11 interactions.<sup>16</sup> When a person visits a website with an embedded pixel, the pixel tracks "events"  
 12 (i.e., user interactions with the site), such as pages viewed, buttons clicked, and information  
 13 submitted.<sup>17</sup> Then, the pixel transmits the event information back to the website server and to third  
 14 parties, where it can be combined with other data and used for marketing.<sup>18</sup>

16 <sup>8</sup> <https://www.bannerhealth.com/> (last acc. Mar. 8, 2024).

17 <sup>9</sup> E.g., search for "chest pain," avail. at  
<https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

18 <sup>10</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

<sup>11</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

19 <sup>12</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

<sup>13</sup> <https://www.bannerhealth.com/calendar> (last acc. Mar. 8, 2024).

20 <sup>14</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).

21 <sup>15</sup> <https://bannerhealth.simplepay.com/app/login> (last acc. Mar. 8, 2024).

22 <sup>16</sup> See Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/>  
 (last accessed Mar. 19, 2023).

23 <sup>17</sup> See Conversion Tracking, META FOR DEVELOPERS,  
<https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking> (last  
 visited May 22, 2023).

<sup>18</sup> *Id.*

1           10. Among the trackers Defendant embedded into its Website is the Facebook Pixel  
2 (also referred to as the “Meta Pixel” or “Pixel”). By default, the Meta Pixel tracks information  
3 about a visitor’s device, including their IP address, and the pages viewed.<sup>19</sup> When configured to  
4 do so, the Meta Pixel can track much more, including a visitor’s search terms, button clicks, and  
5 form submissions.<sup>20</sup> Additionally, the Meta Pixel can link a visitor’s website interactions with an  
6 individual’s unique and persistent Facebook ID (“FID”), allowing a user’s health information to  
7 be linked with their Facebook profile.<sup>21</sup>

8           11. Operating as designed and as implemented by Defendant, the Meta Pixel allowed  
9 Defendant to unlawfully disclose Plaintiff and Class Members’ Private Health Information  
10 alongside identifying details to Facebook. By installing the Meta Pixel on its Website, Defendant  
11 effectively planted a bug on Plaintiff’s and Class Members’ web browsers and compelled them to  
12 disclose Private Information and confidential communications to Facebook without their  
13 authorization or knowledge.

14           12. Facebook encourages and recommends use of its Conversions Application  
15 Programming Interface (“CAPI”) alongside use of the Meta Pixel.<sup>22</sup>  
16

---

17 <sup>19</sup> See Get Started, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/get-started> (last visited May 22, 2023).

18 <sup>20</sup> See Conversion Tracking, META FOR DEVELOPERS,  
19 <https://developers.facebook.com/docs/meta-pixel/implementation/conversion-tracking> (last  
visited May 22, 2023).

20 <sup>21</sup> The Meta Pixel forces the website user to share the user’s FID for easy tracking via the “cookie”  
Facebook stores every time someone accesses their Facebook account from the same web browser.  
“Cookies are small files of information that a web server generates and sends to a web browser.”  
21 “Cookies help inform websites about the user, enabling the websites to personalize the user  
experience.” What are Cookies?, <https://www.cloudflare.com/learning/privacy/what-are-cookies/>  
22 (last visited Jan. 27, 2023).

23 <sup>22</sup> “CAPI works with your Meta Pixel to help improve the performance and measurement of your  
Facebook ad campaigns.” See Samir El Kamouny, How to Implement Facebook Conversions  
API (In Shopify), FETCH & FUNNEL <https://www.fetchfunnel.com/how-to-implement-facebook-conversions-api-in-shopify/> (last visited Jan. 25, 2023).

1           13. Unlike the Meta Pixel, which co-opts a website user's browser and forces it to  
2 transmit information to Facebook in addition to the website owner, CAPI does not cause the user's  
3 browser to transmit information directly to Facebook. Instead, CAPI tracks the user's website  
4 interaction, including Private Information, records and stores that information on the website  
5 owner's servers, and then transmits the data to Facebook from the website owner's servers.<sup>23, 24</sup>

6           14. Indeed, Facebook markets CAPI as a "better measure [of] ad performance and  
7 attribution across your customer's full journey, from discovery to conversion. This helps you better  
8 understand how digital advertising impacts both online and offline results."<sup>25</sup>

9           15. Because CAPI is located on the website owner's servers and is not a bug planted  
10 onto the website user's browser, it allows website owners like Defendant to circumvent any ad  
11 blockers or other denials of consent by the website user that would prevent the Meta Pixel from  
12 sending website users' Private Information to Facebook directly.

13           16. Defendant utilized data from these trackers to market its services and bolster its  
14 profits. Meta Pixel and CAPI are routinely used to target specific customers by utilizing data to  
15 build profiles for the purposes of retargeting and future marketing. Facebook also uses Plaintiff's  
16 and Class Members' Private Information to create targeted advertisements based on the medical  
17 conditions and other information disclosed to Defendant.

18           17. The information that Defendant's Meta Pixel and possibly CAPI sent to Facebook  
19  
20

---

21 <sup>23</sup> What is the Facebook Conversion API and How to Use It, REVEALBOT BLOG,  
<https://revealbot.com/blog/facebook-conversions-api/> (last updated May 20, 2022).

22 <sup>24</sup> "Server events are linked to a dataset ID and are processed like events sent via the Meta  
Pixel.... This means that server events may be used in measurement, reporting, or optimization  
23 in a similar way as other connection channels." Conversions API, META FOR DEVELOPERS,  
<https://developers.facebook.com/docs/marketing-api/conversions-api> (last visited May 15, 2023).

<sup>25</sup> About Conversions API, META FOR DEVELOPERS,  
<https://www.facebook.com/business/help/2041148702652965> (last visited May 15, 2023).

1 can include the Private Information that Plaintiff and Class Members submitted to Defendant's  
2 Website, including details about the pages they browsed and the buttons they clicked, including,  
3 (i) users' keyword searches, (ii) users' physician searches, (iii) content that users viewed;  
4 (iv) activities that reveal the users' status as potential patients; and (v) identifying information.

5 18. Such information allows a third party (e.g., Facebook) to know that a specific  
6 patient was seeking confidential medical care. Facebook, in turn, sells Plaintiff's and Class  
7 Members' Private Information to third-party marketers, who then geotarget Plaintiff's and Class  
8 Members' Facebook pages based on communications obtained via the Meta Pixel and CAPI.  
9 Facebook and any third-party purchasers of Plaintiff's and Class Members' Private Information  
10 also could reasonably infer from the data that a specific patient was being treated for a specific  
11 type of medical condition, such as cancer, pregnancy, dementia, or HIV.

12 19. In addition to the Facebook tracker and CAPI, on information and belief, Defendant  
13 installed other tracking technology which operate similarly to the Meta Pixel and transmit a  
14 website user's Private Information to other third parties.

15 20. Healthcare patients simply do not anticipate that their trusted healthcare provider  
16 will send Personal Health Information ("PHI") or other confidential medical information collected  
17 via its webpages to a hidden third party—let alone Facebook, which has a sordid history of privacy  
18 violations in pursuit of ever-increasing advertising revenue—without the patients' consent.

19 21. Neither Plaintiff nor any Class Member signed a written authorization permitting  
20 Defendant to send their Private Information to Facebook, or any other third parties uninvolved in  
21 their treatment.

22 22. Despite willfully and intentionally incorporating tracking technology, including the  
23 Meta Pixel, potentially CAPI, and other tracking technology such as Google Analytics with Google

1 Tag Manager (“GTM”), Facebook Events, AppDynamics, Taboola, Pinterest, StackAdapt,  
2 LinkedIn, DoubleClick, Skai, Microsoft Universal Events, and Medallia, into its Website and  
3 servers, Banner has never disclosed to Plaintiff or Class Members that it shared their sensitive and  
4 confidential communications and Private Information with third parties including Facebook, and  
5 potentially others.

6 23. Defendant further made express and implied promises to protect Plaintiff’s and  
7 Class Members’ Private Information and maintain the privacy and confidentiality of  
8 communications that patients exchanged with Defendant, including in its privacy policies and  
9 elsewhere.

10 24. Defendant owed common law, statutory, and regulatory duties to keep Plaintiff’s  
11 and Class Members’ communications and Private Information safe, secure, and confidential.

12 25. Upon information and belief, Banner utilized the Meta Pixel and other tracker data  
13 to improve and to save costs on its marketing campaigns, improve its data analytics, attract new  
14 patients, and generate sales.

15 26. Furthermore, by obtaining, collecting, using, and deriving a benefit from Plaintiff’s  
16 and Class Members’ Private Information, Defendant assumed legal and equitable duties to those  
17 individuals to protect and to safeguard that information from unauthorized disclosure.

18 27. Defendant breached its statutory and common law obligations to Plaintiff and Class  
19 Members by, *inter alia*,: (i) failing to adequately review its marketing programs and web based  
20 technology to ensure the hospital Website was safe and secure; (ii) failing to remove or disengage  
21 technology that was known and designed to share web-users’ information; (iii) aiding, agreeing,  
22 and conspiring with third parties to intercept communications sent and received by Plaintiff and  
23 Class Members; (iv) failing to obtain the written consent of Plaintiff and Class Members to

1 disclose their Private Information to Facebook and others; (v) failing to protect Private Information  
2 and take steps to block the transmission of Plaintiff's and Class Members' Private Information  
3 through the use of Meta Pixel and other tracking technology; (vi) failing to warn Plaintiff and Class  
4 Members; and (vii) otherwise failing to design and monitor its Website to maintain the  
5 confidentiality and integrity of patient Private Information.

6 28. Plaintiff seeks to remedy these harms and brings causes of action for  
7 (I) Negligence; (II) Breach of Implied Contract; (III) Unjust Enrichment; (IV) Breach of Fiduciary  
8 Duty; (V) Invasion of Privacy; (VI) Invasion of Privacy under the California Constitution, Cal.  
9 Const. ART. 1 § 1; (VII) Violation of the California Invasion of Privacy Act ("CIPA"), Cal. Penal  
10 Code §§ 630, *et seq.*; (VIII) Violation of the California Confidentiality of Medical Information  
11 Act ("CMIA"), Cal. Civil Code §§ 56.06, 56.10, 56.101; (IX) Violation of the Comprehensive  
12 Computer Data Access and Fraud Act ("CDAFA"), Cal. Penal Code § 502; and, (X) Violation of  
13 Cal. Bus. & Prof. Code §§ 17200, *et. seq.*

#### 14 PARTIES

15 29. Plaintiff, JOHN DOE, is a natural person and a resident and citizen of the State of  
16 California where he intends to remain, with a principal residence in Susanville, California in  
17 Lassen County. He is a patient of Defendant and a victim of Banner's Disclosure of his Private  
18 Information.

19 30. Defendant, BANNER HEALTH ("Banner" or "Defendant"), is a not-for-profit  
20 corporation organized and existing under the laws of the State of Arizona with its principal place  
21 of business at 2901 North Central Avenue, Suite 160, Phoenix, Arizona 85012 in Maricopa  
22 County.

23 31. Defendant's Registered Agent for Service of Process is C T Corporation System,

330 N Brand Boulevard, Suite 700, Glendale, California 91203.

## JURISDICTION & VENUE

32. The Court has personal jurisdiction over Defendant because Banner transacts business in the State of California by providing medical treatment services.

33. This is a class action brought pursuant to Cal. Civ. Proc. Code § 382, and this Court has jurisdiction over the Plaintiff's claims because the amount in controversy exceeds this Court's jurisdictional minimum.

34. Venue is proper under Cal. Civ. Proc. Code § 395(a) because the injury to personal property complained of herein occurred in Lassen County.

## COMMON FACTUAL ALLEGATIONS

### A. Background

35. Founded in 1999 and based on Pheonix, Arizona, Banner is a massive healthcare system which provides treatment services to patients in Arizona, California, Colorado, Nebraska Nevada, Wyoming,<sup>26</sup> and in Alaska, through "28 hospitals and a growing network of health centers and clinics."<sup>27</sup>

36. On its Website, Defendant represents to patients and prospective patients that:

At all stages in life, you can rest assured that Banner will meet your health and medical needs through compassionate professionals and outstanding service. Headquartered in Phoenix, Arizona., Banner Health is one of the largest, nonprofit health care systems in the country and the leading nonprofit provider of hospital services in all the communities we serve.<sup>28</sup>

37. Indeed, Banner owns and operates numerous hospital and medical centers, including: Banner Boswell Medical Center in Sun City, Arizona; Banner Del E Webb Medical

---

<sup>26</sup> See generally, <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

<sup>27</sup> <https://www.bannerhealth.com/about/glance/history> (last acc. Mar. 8, 2024).

<sup>28</sup> <https://www.bannerhealth.com/about> (last acc. Mar. 8, 2024).



Center, in Sun City West Arizona; Banner MD Anderson Cancer Center at Banner Gateway Medical Center, in Gilbert, Arizona; Banner Gateway Medical Center in Gilbert, Arizona; Banner Rehabilitation Hospital West in Peoria, Arizona; Banner Ocotillo Medical Center in Chandler, Arizona; Banner Behavioral Health Hospital in Scottsdale, Arizona; Banner - University Medical Center South in Tucson, Arizona; Banner - University Medical Center Tucson in Tucson, Arizona; Diamond Children's Medical Center in Tucson, Arizona; Banner Thunderbird Medical Center and Banner Children's at Thunderbird in Glendale, Arizona; Banner Payson Medical Center in Payson, Arizona; Banner Children's at Desert in Mesa, Arizona; Banner Desert Medical Center in Mesa, Arizona; Banner Heart Hospital in Mesa, Arizona; Banner Rehabilitation Hospital East and Banner Baywood Medical Center in Mesa, Arizona; Banner Ironwood Medical Center in Queen Creek, Arizona; Banner Goldfield Medical Center in Apache Junction, Arizona; Banner Rehabilitation Hospital Phoenix, Banner Estrella Medical Center, and Banner - University Medical Center Phoenix in Phoenix, Arizona; Page Hospital in Page, Arizona; Banner Lassen Medical Center in Susanville, California; Banner Casa Grande Medical Center in Casa Grande, Arizona; Sterling Regional MedCenter in Sterling, Colorado; Banner Fort Collins Medical Center in Fort Collins, Colorado; Banner North Colorado Medical Center in Greeley, Colorado; East Morgan County Hospital in Brush, Colorado; Banner McKee Medical Center in Loveland, Colorado; Banner Churchill Community Hospital in Fallon, Nevada; Community Hospital in Torrington, Wyoming; Banner Wyoming Medical Center in Casper, Wyoming; Platte County Memorial Hospital in Wheatland, Wyoming; Washakie Medical Center in Worland, Wyoming; Ogallala Community Hospital in Ogallala, Nebraska.<sup>29</sup>

---

<sup>29</sup> See, "Locations," avail. at <https://www.bannerhealth.com/locations?loctype=Hospital&PageNo=1> (last acc. Mar. 8, 2024).

38. One of these facilities is Banner Lassen Medical Center in Susanville, California, originally founded in 1883, “[a] 25-bed, critical access hospital” with a “focus [] to provide you with outstanding care and an excellent patient care experience through the latest in medical technology, a vision of compassion, and a concentration on patient and employee safety [...and...] offer[ing] a wide range of programs and services to aid in prevention, diagnosis and treatment of illness.”<sup>30</sup>

39. Another one of Defendant’s facilities is University Medical Center Tucson, established in 1971, a “non-profit hospital with 649 licensed beds, providing a wide range of inpatient and outpatient services [with] more than 3,000 health care professionals and support staff, and a medical staff of more than 1,300 physicians who serve Tucson and surrounding areas.”<sup>31</sup>

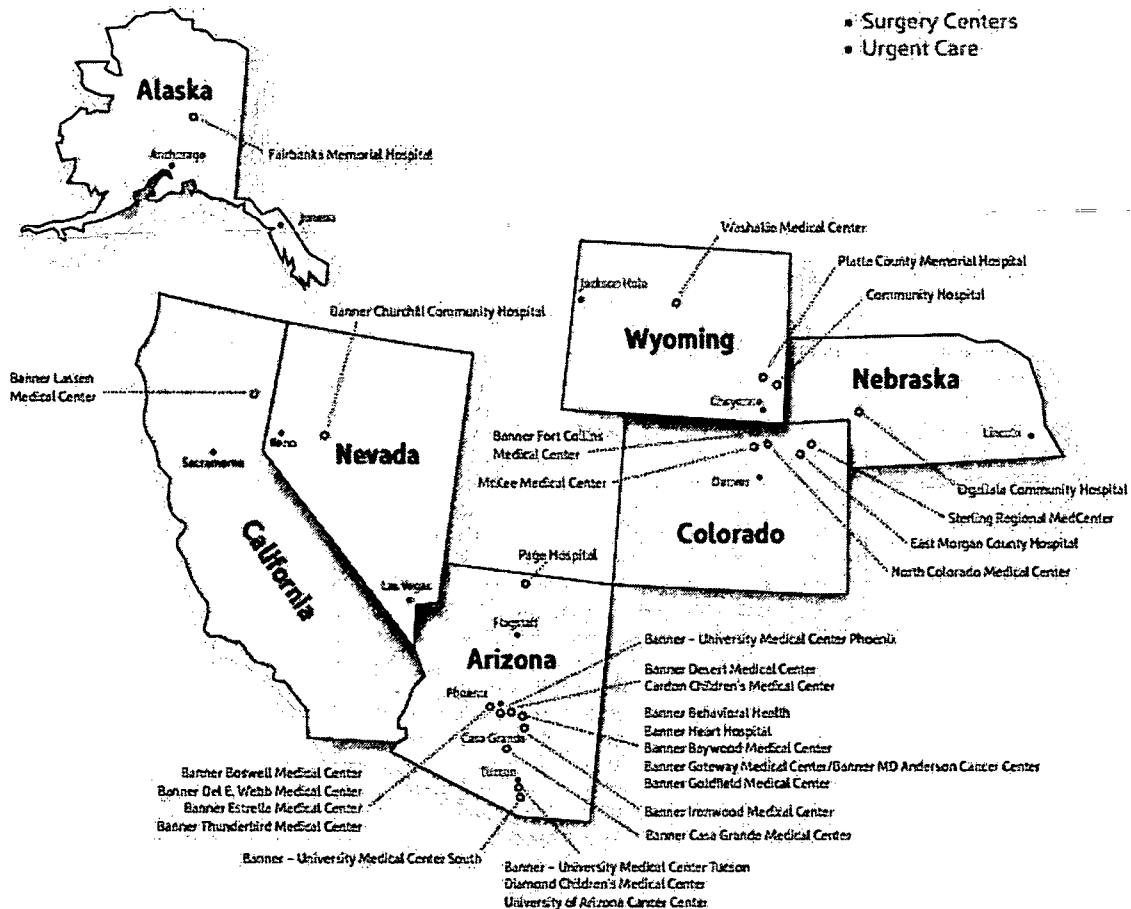
40. Moreover, banner operates hundreds of physicians’ clinics, urgent care clinics, diagnostic imaging practices, physical therapy locations, surgery centers, specialized breast health centers, emergency care departments, as well as home care and equipment locations, laboratories, pharmacies, specialty care centers (e.g., Banner MD Anderson Cancer Center), and other health service locations such as Banner Health schools and senior centers.<sup>32</sup>

<sup>30</sup> <https://www.bannerhealth.com/locations/susanville/banner-lassen-medical-center> (last acc. Mar. 12, 2024).

<sup>31</sup> *Banner Health 2022 CHNA Banner University Medical Center – Tucson Banner University Medical Center – South*, adopted by Banner Health Board of Directors Dec. 9, 2022, pg. 1, avail. at <https://www.bannerhealth.com/-/media/files/project/bh/chna-reports/2022/arizona/banner-university-medical-centers-tucson-and-south-cover-section-tucson.ashx#:~:text=On%20an%20annual%20basis%2C%20Banner,65%2C000%20patients%20in%20the%20ED> (last acc. Mar. 8, 2024).

<sup>32</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

41. As shown on its Website, the scope of Banner's treatment is truly nationwide:<sup>33</sup>



42. At its many medical care facilities, Banner provides myriad medical treatment services, including in areas of: emergency medical care; surgery (including outpatient surgery, general surgery, and neurosurgery); Academic Medicine; Allergy & Immunology; Alzheimer's Disease & Dementia; Asthma; Audiology; Banner Brain & Spine; Bariatric & Weight Loss Surgery; Behavioral & Mental Health; Burn Care; Cancer; Concierge Medicine; Concussion; Critical Care Medicine; Dermatology; Diabetes; Doctors & Specialists; Ear, Nose & Throat;

<sup>33</sup> Banner Health, Fact Sheet, *A leading health care system in the nation*, avail. at <https://www.bannerhealth.com/-/media/files/project/bh/about/history/154267bhgeneralmainfs5115.ashx> (last acc. Mar. 8, 2024).

Endocrinology; Endoscopy; Eye Care; Family Medicine; Gastroenterology; Geriatrics; Gynecology; Healthy Aging; Heart; Home Care; Hospice; Imaging; Infectious Disease; Infusion Therapy; Injury Prevention; Integrative Therapy; Intensive Care; Internal Medicine; Kidney; Labs; Maternity; Medical Imaging; Neonatology; Neurology; Nutrition; Obstetrics; Occupational Health; Orthopedics; Pain Management; Palliative Care; Pediatrics; Pharmacy; Physical Therapy; Poison & Drug Information Center; Primary Care; Psychology; Pulmonary; Rehabilitation; Research; Spine; Sleep Medicine; Sports Medicine; Telehealth; Transplant; Urgent Care; Urology; Women’s Health; and Wound Care.<sup>34</sup>

43. Further, Banner provides specialized treatment through dedicated institutes, including: Banner - University Medicine Heart Institute (“[t]he most current and advanced care for your heart” with a Cardiovascular Intervention Center, Heart Rhythm Disorders Center, and Women’s Heart Center); Banner - University Medicine Neuroscience Institute (“State-of-the-art care for neurological conditions”); Banner - University Orthopedic and Sports Medicine Institute (“[e]xpert care to keep your muscles and joints moving”); and Banner - University Medicine Women’s Institute (“[c]omprehensive care from maternity to menopause”).<sup>35</sup>

44. Banner boasts having over 50,000 employees, being “one of the country’s largest employers [...], [ Arizona’s...] largest private employer, and [] one of Northern Colorado’s largest employers.”<sup>36</sup>

45. Defendant touts that:

Ultimately, Banner’s unwavering commitment to the health and well-being of its communities has earned accolades from an array of industry organizations, Banner Health’s Supply Chain was recognized as second in the nation in 2021, and one of the nation’s Top 10 Integrated Health Systems according to SDI and Modern

<sup>34</sup> <https://www.bannerhealth.com/services/service-listing> (last acc. Mar. 8, 2024).

<sup>35</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

<sup>36</sup> <https://www.bannerhealth.com/about> (last acc. Mar. 8, 2024).

Healthcare Magazine. Banner Alzheimer's Institute has also garnered international recognition for its groundbreaking Alzheimer's Prevention Initiative, brain imaging research and patient care programs. Further, Banner Health, which is the second largest private employer in both Arizona and Northern Colorado, continues to be recognized as one of the "Best Places to Work" by Becker's Hospital Review.<sup>37</sup>

46. In 2023, Defendant generated annual revenue approximating \$7.8 billion.<sup>38</sup>

47. Banner serves many of its patients via its Online Platforms, which it encourages patients to use to learn about Banner on its main homepage,<sup>39</sup> to search for health information,<sup>40</sup> to find a doctor,<sup>41</sup> to find locations,<sup>42</sup> to learn about medical conditions and treatment services,<sup>43</sup> to learn about classes and events,<sup>44</sup> to access a patient portal,<sup>45</sup> to pay bills,<sup>46</sup> and more.

48. In furtherance of its goal of increasing sales and profitability, and to improve the success of its advertising and marketing, Defendant purposely installed the Meta Pixel and other trackers, such as Google Analytics with Google Tag Manager ("GTM"), Facebook Events, AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal Events, and Medallia onto its Website, for the purpose of gathering information about Plaintiff and Class Members to further its marketing efforts. But Defendant did not only generate information

<sup>37</sup> *Banner Health 2022 CHNA Banner University Medical Center – Tucson Banner University Medical Center – South*, adopted by Banner Health Board of Directors Dec. 9, 2022, pg. 1, avail. at <https://www.bannerhealth.com/-/media/files/project/bh/chna-reports/2022/arizona/banner-university-medical-centers-tucson-and-south-cover-section-tucson.ashx#:~:text=On%20an%20annual%20basis%2C%20Banner.65%2C000%20patients%20in%20the%20ED> (last acc. Mar. 8, 2024).

<sup>38</sup> <https://www.zippia.com/banner-health-careers-61932/revenue/> (last acc. Mar. 8, 2024).

<sup>39</sup> <https://www.bannerhealth.com/> (last acc. Mar. 8, 2024).

<sup>40</sup> E.g., search for "chest pain," avail. at <https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

<sup>41</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

<sup>42</sup> <https://www.bannerhealth.com/find-a-location> (last acc. Mar. 8, 2024).

<sup>43</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

<sup>44</sup> <https://www.bannerhealth.com/calendar> (last acc. Mar. 8, 2024).

<sup>45</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).

<sup>46</sup> <https://bannerhealth.simplepay.com/app/login> (last acc. Mar. 8, 2024).

1 for its own use: it also shared patient information, including Private Information belonging to  
2 Plaintiff and Class Members, with Facebook and other unauthorized third parties.

3 49. To better understand Defendant's unlawful data-sharing practices, a brief  
4 discussion of basic web design and tracking tools follows.

5 *i. Facebook's Business Tools and the Meta Pixel*

6 50. Facebook operates the world's largest social media company and generated \$117  
7 billion in revenue in 2021, roughly 97% of which was derived from selling advertising space.<sup>47</sup>

8 51. In conjunction with its advertising business, Facebook encourages and promotes  
9 entities and website owners, such as Defendant, to utilize its "Business Tools" to gather, identify,  
10 target, and market products and services to individuals.

11 52. Facebook's Business Tools, including the Meta Pixel and Conversions API, are bits  
12 of code that advertisers can integrate into their webpages, mobile applications, and servers, thereby  
13 enabling the interception and collection of user activity on those platforms.

14 53. The Business Tools are automatically configured to capture "Standard Events" such  
15 as when a user visits a particular webpage, the webpage's Universal Resource Locator ("URL"),  
16 as well as metadata, button clicks, and other information.<sup>48</sup> Businesses that want to target  
17 customers and advertise their services, such as Defendant, can track other user actions and can  
18

19  
20 <sup>47</sup> Meta Reports Fourth Quarter and Full Year 2021 Results, FACEBOOK  
<https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx> (last visited Nov. 14, 2022).

21 <sup>48</sup> Specifications for Facebook Pixel Standard Events, META,  
<https://www.facebook.com/business/help/402791146561655> (last visited Jan. 31, 2023); *see also*  
22 Facebook Pixel, Accurate Event Tracking, Advanced, META FOR DEVELOPERS;  
<https://developers.facebook.com/docs/facebook-pixel/advanced/>; *see also* Best Practices for  
23 Facebook Pixel Setup, META <https://www.facebook.com/business/help/218844828315224>; App  
Events API, META FOR DEVELOPERS, [https://developers.facebook.com/docs/marketing-api/app-](https://developers.facebook.com/docs/marketing-api/app-event-api/)  
event-api/ (last visited Jan. 31, 2023).

1 create their own tracking parameters by building a “custom event.”<sup>49</sup>

2 54. One such Business Tool is the Meta Pixel, a tool that “tracks the people and type  
3 of actions they take.”<sup>50</sup> When a user accesses a webpage that is hosting the Meta Pixel, the  
4 communications with the host webpage are instantaneously and surreptitiously duplicated and sent  
5 to Facebook—traveling from the user’s browser to Facebook’s server.

6 55. Notably, this transmission only occurs on webpages that contain the Pixel. A  
7 website owner can configure its website to use the Pixel on certain webpages that don’t implicate  
8 patient privacy (such as the homepage) and disable it on pages that do implicate patient privacy  
9 (such as Defendant’s “Services” pages<sup>51</sup>).

10 56. The Meta Pixel’s primary purpose is for marketing and ad targeting and sales  
11 generation.<sup>52</sup>

12 57. Facebook’s own website informs companies that “[t]he Meta Pixel is a piece of  
13 code that you put on your website that allows you to measure the effectiveness of your advertising  
14 by understanding the actions people take on your website.”<sup>53</sup>

15 58. According to Facebook, the Meta Pixel can collect the following data.

16 **Http Headers** – Anything present in HTTP headers. HTTP Headers are a standard  
17 web protocol sent between any browser request and any server on the internet.  
18 HTTP Headers include IP addresses, information about the web browser, page  
19 location, document, referrer and *person using the website*. (emphasis added).

**Pixel-specific Data** – Includes Pixel ID and the Facebook Cookie.

20 <sup>49</sup> About Standard and Custom Website Events, META,  
21 <https://www.facebook.com/business/help/964258670337005>; *see also* Facebook, App Events  
22 API, *supra*.

<sup>50</sup> Retargeting, META, <https://www.facebook.com/business/goals/retargeting>.

<sup>51</sup> <https://pamhealth.com/health-services> (last acc. Mar. 6, 2024).

<sup>52</sup> *See* Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/>  
23 (last accessed Mar. 19, 2023).

<sup>53</sup> About Meta Pixel, META,  
<https://www.facebook.com/business/help/742478679120153> (last accessed Mar. 19, 2023).



1 **Button Click Data** – Includes any buttons clicked by site visitors, the labels those  
2 buttons and any pages visited as a result of the button clicks.

3 **Optional Values** – Developers and marketers can optionally choose to send  
4 additional information about the visit through Custom Data events. Example  
5 custom data events are conversion value, page type and more.

6 **Form Field Names** – Includes website field names like email, address, quantity,  
7 etc., for when you purchase a product or service. We don't capture field values  
8 unless you include them as part of Advanced Matching or optional values.<sup>54</sup>

9 59. Facebook boasts to its prospective users that the Meta Pixel can be used to:

- 10 • **Make sure your ads are shown to the right people.** Find new customers,  
11 or people who have visited a specific page or taken a desired action on your  
12 website.
- 13 • **Drive more sales.** Set up automatic bidding to reach people who are more  
14 likely to take an action you care about, like making a purchase.
- 15 • **Measure the results of your ads.** Better understand the impact of your ads  
16 by measuring what happens when people see them.<sup>55</sup>

17 60. Facebook likewise benefits from the data received from the Meta Pixel and uses the  
18 data to serve targeted ads and identify users to be included in such targeted ads.

19 *ii. Defendant's method of transmitting Plaintiff's and Class Members' Private*  
20 *Information via the Meta Pixel and/or Conversions API i.e., the Interplay between*  
21 *HTTP Requests and Responses, Source Code, and the Meta Pixel*

22 61. Web browsers are software applications that allow consumers to navigate the  
23 internet and view and exchange electronic information and communications. Each "client device"  
(such as computer, tablet, or smart phone) accesses web content through a web browser (e.g.,  
Google's Chrome browser, Mozilla's Firefox browser, Apple's Safari browser, and Microsoft's  
Edge browser).

<sup>54</sup> Meta Pixel, META FOR DEVELOPERS, <https://developers.facebook.com/docs/meta-pixel/> (last accessed Mar. 19, 2023).

<sup>55</sup> About Meta Pixel, META, <https://www.facebook.com/business/help/742478679120153> (last accessed Mar. 19, 2023).

1           62. Every website is hosted by a computer “server” that holds the website’s contents  
2 and through which the website owner exchanges files or communications with Internet users’  
3 client devices via their web browsers.

4           63. Web communications consist of HTTP Requests and HTTP Responses, and any  
5 given browsing session may consist of thousands of individual HTTP Requests and HTTP  
6 Responses, along with corresponding cookies.<sup>56</sup>

7           64. GET Requests are one of the most common types of HTTP Requests. In addition  
8 to specifying a particular URL (i.e., web address), they also send the host server data, which is  
9 embedded inside the URL and can include cookies.

10          65. When an individual visits a website, their web browser sends an HTTP Request to  
11 the entity’s servers that essentially asks the website to retrieve certain information (such as  
12 Defendant’s search function page). The entity’s servers send the HTTP Response, which contains  
13 the requested information in the form of “Markup.” This is the foundation for the pages, images,  
14 words, buttons, and other features that appear on the patient’s screen as they navigate a website.

15          66. Every website is comprised of Markup and “Source Code.” Source Code is simply  
16 a set of instructions that commands the website visitor’s browser to take certain actions when the  
17 web page first loads or when a specified event triggers the code.

18          67. Source code may also command a web browser to send data transmissions to third  
19 parties in the form of HTTP Requests quietly executed in the background without notifying the  
20 web browser’s user.

21  
22  
23 

---

<sup>56</sup>“Cookies are small files of information that a web server generates and sends to a web browser . . . Cookies help inform websites about the user, enabling the websites to personalize the user experience.” <https://www.cloudflare.com/learning/privacy/what-are-cookies/> (last visited Jan. 27, 2023).

1           68. Defendant's implementation of the Meta Pixel is source code that acted much like  
2 a traditional wiretap, intercepting and transmitting communications intended only for Defendant.

3           69. Separate from the Meta Pixel, Facebook and other website owners can place third-  
4 party cookies in the web browsers of users logged into their websites or services. These cookies  
5 can uniquely identify the user so the cookie owner can track the user as he moves around the  
6 internet—whether on the cookie owner's website or not. Facebook uses this type of third-party  
7 cookie when Facebook account holders use the Facebook app or website. As a result, when a  
8 Facebook account holder uses Defendant's Website, the account holder's unique Facebook ID is  
9 sent to Facebook, along with the intercepted communication, allowing Facebook to identify the  
10 patient associated with the Private Information it has intercepted.

11           70. With substantial work and technical know-how, internet users can sometimes  
12 circumvent this browser-based wiretap technology. To counteract this, third parties bent on  
13 gathering data and Private Information implement workarounds that are difficult to detect or evade.  
14 Facebook's workaround is its Conversions API tool, which is particularly effective because the  
15 data transmitted via this tool does not rely on the website visitor's web browsers. Rather, the  
16 information travels directly from the entity's server to Facebook's server.

17           71. Conversions API "is designed to create a direct connection between [web hosts']  
18 marketing data and [Facebook]."<sup>57</sup> Thus, the entity receives and stores its communications with  
19 patients on its server before Conversions API collects and sends those communications—and the  
20 Private Information contained therein—to Facebook.

21           72. Notably, client devices do not have access to host servers and thus cannot prevent  
22  
23

---

<sup>57</sup> About Conversions API, META, <https://www.facebook.com/business/help/2041148702652965> (last visited May 15, 2023).

1 (or even detect) this additional transmission of information to Facebook.

2 73. While there is no way to confirm with certainty that a website owner is using  
3 Conversions API without accessing the host server, Facebook instructs companies like Defendant  
4 to “[u]se the Conversions API in addition to the Meta Pixel, and share the same events using both  
5 tools,” because such a “redundant event setup” allows the entity “to share website events [with  
6 Facebook] that the pixel may lose.”<sup>58</sup> Thus, if an entity implemented the Meta Pixel in accordance  
7 with Facebook’s documentation, it is also reasonable to infer that it implemented the Conversions  
8 API tool on its Website.

9 74. The third parties to whom a website transmits data through pixels and other tracking  
10 technology do not provide any substantive content on the host website. In other words, Facebook  
11 and others like it are not providing anything to the user relating to the user’s communications.  
12 Instead, these third parties are typically procured to track user data and communications only to  
13 serve the marketing purposes of the website owner (i.e., to bolster profits).

14 75. Accordingly, without any knowledge, authorization, or action by a user, a website  
15 owner like Defendant can use its source code to commandeer its patients’ computing devices,  
16 causing the device’s web browser to contemporaneously and invisibly re-direct the patients’  
17 communications to hidden third parties like Facebook.

18 76. In this case, Defendant employed the Meta Pixel and potentially Conversions API  
19 to intercept, duplicate, and re-direct Plaintiff’s and Class Members’ Private Information to  
20 Facebook contemporaneously, invisibly, and without the patient’s knowledge.

21  
22  
23  

---

<sup>58</sup> See Best Practices for Conversions API, META,  
<https://www.facebook.com/business/help/308855623839366> (last visited May 15, 2023).

1           77. Consequently, when Plaintiff and Class Members visited Defendant's Website and  
2 communicated their Private Information, it was simultaneously intercepted and transmitted to  
3 Facebook.

4           78. On information and belief, Banner also employed other trackers, such Google  
5 Analytics with Google Tag Manager ("GTM"), Facebook Events, AppDynamics, Taboola,  
6 Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal Events, and Medallia,  
7 which likewise transmitted Plaintiff's and the Class Members' Private Information to third parties  
8 without Plaintiff's and Class Members' knowledge or authorization.

9           *iii. Defendant Violated its own Privacy Policies*

10           79. Banner maintains and is covered under privacy policies, including a Notice of  
11 Privacy Practices,<sup>59</sup> a Website Privacy Statement,<sup>60</sup> and a Website Terms of Use,<sup>61</sup> which are  
12 posted on Defendant's Website (collectively "Privacy Policies").

13           80. In its Notice of Privacy Practices, Defendant represents, acknowledges, and  
14 promises:

15           **Banner is committed to protecting the confidentiality of information about you**  
16 **and is required by law to do so.** This notice describes how we may use  
17 information about you within Banner Health and how we may disclose it to others  
18 outside Banner. **We will notify you if there is a breach of your unsecured**  
19 **protected health information.** This notice also describes the rights you have  
20 concerning your own health information.<sup>62</sup>

21 <sup>59</sup> Banner Health, *Notice of Privacy Practices*, effective date September 23, 2023, available at  
22 <https://www.bannerhealth.com/-/media/files/project/bh/patients-visitors/privacy-practices/hipaa-eng-fs-03-28-19.ashx> (last acc. Mar. 8, 2024), **attached as Exhibit B.**

23 <sup>60</sup> Banner Health, *Privacy Statement*, last updated November 2019, avail. at  
<https://www.bannerhealth.com/about/legal-notices/privacy> (last acc. Mar. 8, 2024), **attached as Exhibit C.**

<sup>61</sup> Banner Health, *Terms of Use*, avail. at <https://www.bannerhealth.com/about/legal-notices/terms> (last acc. Mar. 8, 2024), **attached as Exhibit D.**

<sup>62</sup> *Notice of Privacy Practices*, **Exhibit B** (emphases added).

1           81.     Therein, Banner further specifically represents, acknowledges, and promises that  
 2 except as provided in the Notice of Privacy Practices, “[o]ther uses and disclosures not  
 3 described in this notice will be made only with your written authorization, such as sale of  
 4 medical information. You may revoke such an authorization by sending us a written request.”<sup>63</sup>

5           82.     Indeed, Banner’s Notice of Privacy Practices enumerates specific purposes for  
 6 which it may disclose PHI/Private Information, including for: treatment (“Banner may use  
 7 information about you to provide you with medical services and supplies. We may also disclose  
 8 information about you to others that need the information to treat you, such as doctors, physician  
 9 assistants, nurses, medical and nursing students, technicians, therapists, emergency service and  
 10 medical transportation providers, medical equipment providers, and others involved in your  
 11 care.”); in a Facility Directory; to family members and others involved in patient care; to effectuate  
 12 payment for services; for health care operations (“Banner may use and disclose information about  
 13 you if it is necessary to improve the quality of care we provide to patients or for health care  
 14 operations. We may use information about you to conduct quality improvement activities, to obtain  
 15 audit, accounting, or legal services, or to conduct business management and planning. For  
 16 example, we may use medical information to review our treatment and services and to evaluate  
 17 the performance of our staff in caring for you.”); for fundraising; for research; as required by law  
 18 (“Federal, state, or local laws do not require patient consent to disclose information that is required  
 19 to be reported. For instance, we are required to report child abuse and neglect, gunshot wounds,  
 20 etc. Public policy has determined that these types of needs outweigh the patient’s right to privacy.  
 21 Banner is also required to give information to the state workers’ compensation program for work-  
 22 related injuries.”); for public health purposes; in limited circumstances for public safety; in

---

23 <sup>63</sup> *Id.* (bold emphasis added).

1 connection with Health Oversight Activities; to coroners, medical examiners, and funeral  
2 directors; in connection with organ and tissue donations; for military veterans, national security,  
3 and other government purposes; and in judicial proceedings, subject to certain requirements.<sup>64</sup>

4 83. None of the above purposes enumerated in Banner's Notice of Privacy Practices,  
5 for which it may disclose patients' health information/PHI/Private Information without written  
6 authorization, include Defendant disclosing that information to third-parties uninvolved in their  
7 treatment for marketing purposes.

8 84. Further, Defendant maintains a Privacy Statement, applicable to its Website, in  
9 which Banner states is applicable:

10 ... to the information we collect from you when you use voice, mobile device and  
11 desktop Banner Health platforms, tools and applications, BannerHealth.com and  
12 other Banner Health websites (collectively the "Services"), how we use that  
13 information, and when we disclose it. It will also give you more information about  
14 how to manage the personal information that you provide to us through the  
15 Services. This statement applies only to information you provide to us online while  
16 visiting or using our Services. It does not apply to information we have obtained or  
17 may obtain offline through other traditional means.<sup>65</sup>

18 85. In its Website Privacy Statement, Banner explains the information it collects from  
19 the Online Platforms, including "Automatically Collected Information" or "information []  
20 automatically received and sometimes collected from you when you use the Services [...]  
21 includ[ing] some or all of the following items: the name of the domain and host from which you  
22 access the Internet, including the Internet protocol (IP) address of the computer you are using and  
23 the IP address of your Internet Service Provider; the type and version of Internet browser software  
you use and your operating system; the type and version of your media player(s); the date and time  
you access our Services, the length of your stay and the specific pages, images, video or forms that

---

<sup>64</sup> *Id.*

<sup>65</sup> *Privacy Statement, Exhibit C.*



1 you access while using the Services; the Internet address of the website from which you linked  
 2 directly to our Services and, if applicable, the search engine that referred you and any search strings  
 3 or phrases that you entered into the search engine to find the Services; and demographic  
 4 information concerning the country of origin of your computer and the language(s) used by it.”<sup>66</sup>

5 86. Further, therein, Banner explains that it collects information via cookies, stating:

6 "Cookies" are small files or records that we place on your computer's hard drive to  
 7 distinguish you from other visitors using the Services. The use of cookies is a  
 8 standard practice among websites to collect or track information about your  
 9 activities while using the Services. Some websites use persistent cookies, which are  
 10 placed on your computer and remain there until you delete them. Others use  
 11 temporary cookies, which expire after some period or become overwritten by other  
 12 data. **Banner Health Services use "session cookies" which disappear from your  
 13 computer after you have closed your Internet browser.**

14 Most people do not know that cookies are being placed on their computers when  
 15 they use Banner Health Services or most other websites because browsers are  
 16 typically set to accept cookies. You can choose to have your browser warn you  
 17 every time a cookie is being sent to you or you can turn off cookie placements. If  
 18 you refuse cookies, you can still use Banner Health Services, but your overall  
 19 experience may be affected and some functionality may be reduced or  
 20 unavailable.<sup>67</sup>

21 87. Lastly, in the Privacy Statement, Defendant explains that it collects information  
 22 Website users actively submit when they “(i) submit a job application; (ii) make an online  
 23 donation; (iii) sign up for a class or event conducted at one of our medical centers; (iv) send an e-  
 mail message to us or otherwise provide online comments, criticisms, suggestions or feedback; (v)  
 participate in a chat session; (vi) purchase merchandise from the Banner Store; (vii) reserve a spot  
 or make an appointment at a Banner Health facility; or (viii) pre-register for a hospital procedure  
 such as surgery.”<sup>68</sup>

---

<sup>66</sup> *Id.*

<sup>67</sup> *Id.* (bold emphasis added).

<sup>68</sup> *Id.*

1           88. In its Privacy Statement, Defendant specifically delineates how it uses and shares  
2 Private Information, *to wit*:

- 3           • To process, complete or otherwise act upon or respond to your  
4 request or reason for submitting that information;
- 5           • To register and/or verify you in connection with a service or feature  
6 that you are attempting to access or obtain;
- 7           • To communicate with you about your request or reason for  
8 submitting that information;
- 9           • To provide additional information to you about Banner Health and  
10 its services that we believe may interest you;
- 11           • To study and analyze the use of the information and features  
12 available on our Services; and
- 13           • To assist, when necessary, in protecting our rights or property,  
14 enforcing the provisions of our Privacy Statement and Terms of Use,  
15 and/or preventing harm to you or others.<sup>69</sup>

16           89. None of the above-described purposes enumerated in Banner’s Privacy Statement  
17 include the disclosure of Private Information to third parties uninvolved in patients’ treatment for  
18 marketing purposes, without their authorization, as occurred in the Disclosure.

19           90. Moreover, in its Privacy Statement, Defendant specifically represents,  
20 acknowledges, and promises that, “*We do not sell User Information to third parties*. And except  
21 where we otherwise obtain your express permission, we share your User Information with third  
22 parties only under the limited circumstances stated, including: credit card authorizations, “to  
23 process a particular request you have made, to complete a purchase order for merchandise and to  
deliver your purchase to you or to process a donation[;]” “[...]to conduct background checks,  
obtain credit reports, verify prior employment, check references and for any other lawful purpose  
that is in our judgment reasonably necessary to our interviewing and hiring process; “...in response  
to judicial or other governmental subpoenas, warrants and court orders served on Banner Health

---

<sup>69</sup> *Id.*

1 in accordance with their terms, or as otherwise required by applicable law[;]" "to protect our rights  
 2 or property, to enforce the provisions of our Privacy Statement and Terms of Use, and/or to prevent  
 3 harm to you or others[;]" "...if Banner Health or its business is sold or offered for sale to another  
 4 company or person(s), if a petition for relief under the United States Bankruptcy Laws is filed by  
 5 or against Banner Health, or if Banner Health becomes subject to an order of appointment of a  
 6 trustee or receiver[;]" and sharing user correspondence and information provided in user emails  
 7 "with employees, volunteers, representatives, or agents most capable of addressing your  
 8 correspondence" if users communicate via email.<sup>70</sup>

9 91. Nothing in Defendant's Website Privacy Statement discloses Banner's use of the  
 10 Meta Pixel or related tracking technology, and that users' and patients' Private Information will  
 11 be disclosed to third parties uninvolved in patient's treatment, without their authorization.

12 92. Finally, Defendant maintains a Website Terms of Use, which states, "[b]y  
 13 accessing, using or downloading in any way, without limitation, any materials from this Website  
 14 or merely browsing this Website, you agree to and are bound by these Terms of Use."<sup>71</sup>

15 93. Banner's Website Terms of Use provides:

16 **Banner Health respects the privacy of visitors to our Website. Please see**  
 17 **Banner Health's Privacy Statement relating to the collection and use of your**  
 18 **information. User acknowledges and agrees that this Privacy Statement,**  
 19 **including but not limited to the manner that Banner Health collects, uses and**  
 20 **discloses User's personally identifiable information, is incorporated and made**  
 21 **part of these Terms of Use. If User does not agree to Banner Health's Privacy**  
 22 **Statement, then User should not use this Website or submit or post any personally**  
 23 **identifiable information on this Website. Questions regarding privacy issues should**  
 be directed to Banner Health System Web Services.<sup>72</sup>

---

<sup>70</sup> *Id.* (italics in original).

<sup>71</sup> *Terms of Use*, **Exhibit D**.

<sup>72</sup> *Id.* (bold emphasis added).

1           94. In addition, in its Website Terms of Use, Banner “reserves the right to monitor all  
2 network traffic to this Website to identify and/or block unauthorized attempts or intrusions to  
3 upload or change information or cause damage to this Website in any fashion. Anyone using this  
4 Website expressly consents to such monitoring.”<sup>73</sup>

5           95. Nothing in the Website Terms of Use discloses Banner’s use of the Meta Pixel or  
6 related tracking technology, and that users’ and patients’ Private Information will be disclosed to  
7 third parties uninvolved in patient’s treatment, without their authorization.

8           96. Despite these express, specific representations and promises in its Privacy Policies,  
9 Banner does indeed transfer Private Information to third parties. Using the Meta Pixel, Defendant  
10 used and disclosed Plaintiff’s and Class Member’s Private Information and confidential  
11 communications to Facebook, and other unauthorized third parties, without written authorization,  
12 in violation of Banner’s Privacy Policies.

13           ***iv. Banner Unauthorizedly Disclosed Plaintiff’s and the Class’s Private Information***

14           97. Defendant disclosed Plaintiff’s and Class Members’ Private Information and  
15 confidential communications to third parties for marketing purposes, including Facebook, and  
16 potentially others, including Google Analytics with Google Tag Manager (“GTM”),  
17 AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, Skai, Microsoft Universal Events, and  
18 Medallia, without Plaintiff’s and Class Members’ authorization.

19           98. Through its use of the Meta Pixel, Banner disclosed to Facebook Plaintiff’s and  
20 Class Members’ Private Information communicated via its Website, including details about the  
21 pages they browsed and the buttons they clicked, including (i) users’ keyword searches, (ii) users’  
22 physician searches, (iii) content that users viewed, and (iv) activities that reveal the users’ status  
23

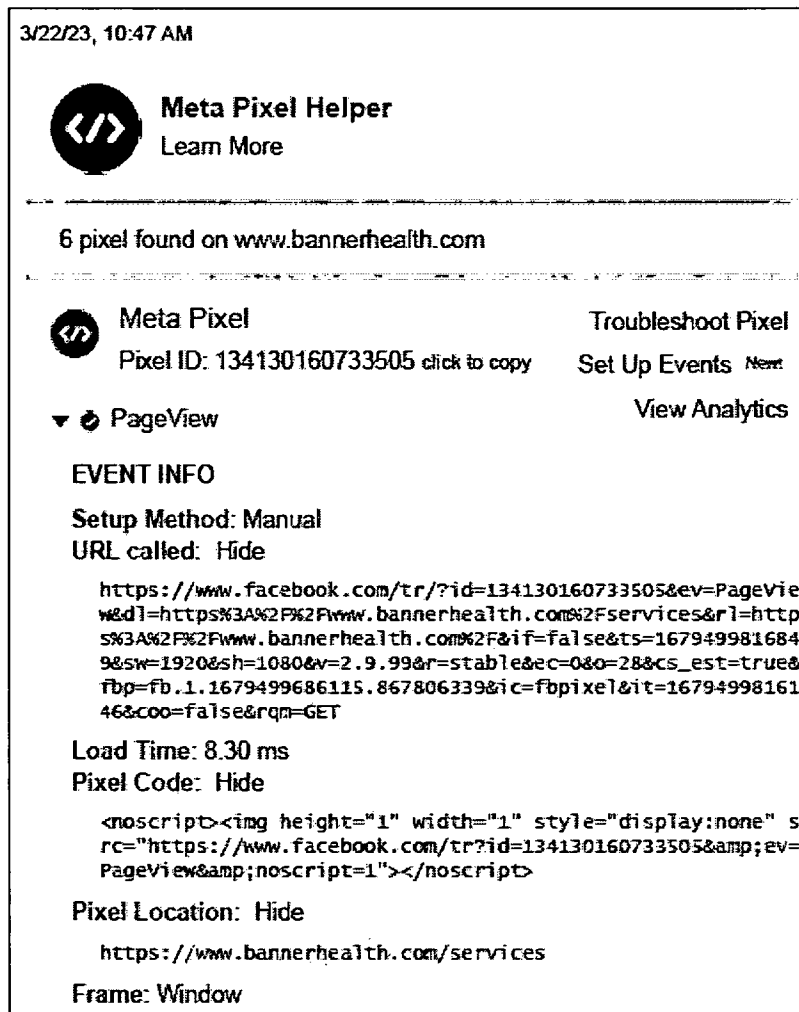
---

<sup>73</sup> *Id.*

as potential patients.

99. In addition to this information, (v) the Meta Pixel collects and transmits to Facebook other identifying information, including IP addresses, and users' "c\_user" cookies, which Facebook uses to identify users, and are transmitted in Meta Pixel events. Therefore, the Meta Pixel events Banner sent likely allowed Facebook to connect users' identities with the details reported within the events.

100. For example, Banner installed Meta Pixels on its pages for medical services:<sup>74</sup>



<sup>74</sup> <https://www.bannerhealth.com/services> (last acc. Mar. 8, 2024).

1 101. As of October 2023, Banner had multiple Meta Pixels installed on its Website with  
2 the following IDs: 534707753606264 (“Pixel1”); 354902315267014 (“Pixel2”);  
3 876783143355083 (“Pixel3”); 317691905318614 (“Pixel4”); 134130160733505 (“Pixel5”); and  
4 352572695583032 (“Pixel6”).

5 102. Even prior to that time, as of March 30, 2021, Banner had three additional Meta  
6 Pixels with IDs: 200525233628970 (“Pixel7”); 375127919853316 (“Pixel8”); and (9)  
7 499798837564477 (“Pixel9”). Further, there are three GTM accounts with IDs GTM-P6NQWFD  
8 (“GTM1”), GTM-K8Z9P6T (“GTM2”), and GTM-NSPWG36 (“GTM3”).

9 Banner Disclosed Users’ Keyword Searches

10 103. Banner shared information with Facebook about users’ searches through  
11 PageView, Microdata, and SubscribedButtonClick events.

12 104. Upon users’ arrival on Banner’s homepage, Banner sent PageView and Microdata  
13 events informing Facebook that the user was on “.” The Microdata event also provides that Banner  
14 offers healthcare in “AZ, CO, WY, NE, NV, CA” and that the user can “Find a provider, schedule  
15 an appointment, or find the nearest Banner Health location near you.”

16 105. As users moved beyond the homepage, Banner continued to report users’ activities  
17 to Facebook.

18 106. If that was not bad enough, Defendant sent Facebook Plaintiff’s and the Class  
19 Members’ search query information. For example, when a user searched for the keyword “cancer,”  
20 Banner reported that activity to Facebook through SubscribedButtonClick, PageView and  
21 Microdata events, which all disclosed the user’s “query=cancer.”

22 107. The SubscribedButtonClick event includes additional information about the user’s  
23 specific activities, such as that the user clicked a button labeled “Search” connected to a form that

1 allows the user to “Search for doctors, locations, services, and more.”

2 108. With the search results displayed, the user may refine their search results by  
3 displaying the results by categories such as all results, locations results, or services results only.  
4 Banner also reported this type of activity. For example, if the user clicked to display all results,  
5 Banner sent a SubscribedButtonClick event, revealing that the user clicked on a button labeled  
6 “SERVICES” on a page titled “Banner Health Search Results” and that the user navigated to that  
7 page by searching “query=cancer.”

8 Banner Disclosed Users’ Physician Search Activities

9 109. Banner informed Facebook when users searched for physicians on the Banner  
10 website through SubscribedButtonClick, PageView, and Microdata events.

11 110. Banner sent a SubscribedButtonClick event as soon as a user navigated to Banner’s  
12 Find A Doctor page.

13 111. The SubscribedButtonClick disclosed that the user clicked a button labeled “Find a  
14 Doctor” and that the user navigated to the user’s current page after viewing a page on  
15 “<https://www.bannerhealth.com/services/cancer>.”

16 112. Upon the user loading the Find a Doctor page, Banner sent a pair of PageView and  
17 Microdata events, confirming that the user landed on the page with a “physician-directory” for the  
18 user to “Find a Doctor near you.”

19 113. Finally, as the user clicked to search for an oncology physician, Banner sent another  
20 SubscribedButtonClick event, informing Facebook that the user clicked “Search” to “Find a  
21 Doctor.”  
22  
23



Banner Disclosed Content That Users Viewed

114. Additionally, Defendant shared information as to the contents of its Website pages which Website users viewed. Banner disclosed information about content that users viewed through PageView, Microdata, and SubscribedButtonClick events.

115. For instance, when a user clicked to view “Classes + Events,” Banner reported that via a SubscribedButtonClick event. When the user arrived on Banner’s calendar page for its classes and events, Banner sent a pair of PageView and Microdata events, disclosing that the user was looking at the “/calendar” page.

116. Banner continued to share the user’s activities as the user clicked on specific classes. For instance, when the user clicked to view more about a diabetes class, Banner reported that the user clicked a button labeled “Dial Into Diabetes: Nutrition Basics and Medication Management- Virtual” while the user was on the “Calendar” page.

117. When the Dial Into Diabetes information page loaded, Banner sent another pair of PageView and Microdata events. The Microdata event reveals the user’s potential health insurance status due to the fact that the event indicates the user must be insured by “Banner Medicare Advantage (Dual, HMO, PPO) in order to register for the class.”

118. Additionally, the Microdata event reveals more information about the Dial Into Diabetes class too, including the time and date of the event, e.g., “11/01/2023, 10:00 am,” and the modality of the class via “Microsoft Teams Meeting.”

119. Then, Banner disclosed the user’s registration for the class through a series of SubscribedButtonClick, PageView, and Microdata events.

120. As another illustration of Banner’s disclosures of content that users viewed, Banner transmitted a series of SubscribedButtonClick, PageView, and Microdata events as the user took

1 a heart health risk assessment on Banner's website.

2 121. Banner began reporting about the user's health risk assessment activities when the  
3 user clicked to view Banner's offered health risk assessments. As the user clicked to browse the  
4 offered assessments, Banner sent a SubscribedButtonClick event.

5 122. When the page loaded, Banner then sent a pair of PageView and Microdata events,  
6 informing Facebook that the user can take "free health risk assessments" to "learn about your risk  
7 as well as stay informed about your health."

8 123. Next, when the user loaded a page for the heart health risk assessment, Banner  
9 transmitted PageView and Microdata events, revealing that the user was viewing a "Heart Age  
10 Test" which allows the user to "Estimate your risk of heart and blood vessel disease."

11 124. As the user clicked to start the assessment, progressed through each question, and  
12 then completed the assessment, Banner sent a mixture of SubscribedButtonClick, Pageview, and  
13 Microdata events sharing the user's progress with Facebook.

14 Banner Discloses Users' Activities That Reveal Their Status as Potential Patients

15 125. Further still, Banner discloses Users' activities that reveal their status as potential  
16 patients. Through PageView, Microdata, and SubscribedButtonClick events, Banner disclosed  
17 information about users' activities that reveal their status as potential patients.

18 126. For example, when the user clicked to access the Patient Account page, Banner sent  
19 a SubscribedButtonClick event disclosing that the user clicked a button labeled "Patient Account"  
20 on a page titled "Patients & Visitors | Banner Health." Banner further sent PageView and  
21 Microdata events, informing Facebook that the user was now on the Patient Account page, which  
22 "offers 24/7 online access to your health information."

23 127. From the Patient Account page, the user could either click to create a patient

1 account or click to sign into their patient account. Both activities triggered a  
2 SubscribedButtonClick event, disclosing that the user was on the “/patient-account” page and that,  
3 either, the user clicked a button for “Creating an Account” or to “Sign In,” respectively.

4 128. In addition to Banner sharing information with Facebook about users’ patient  
5 account-related activities, Banner also sent events with data about users’ activities related to  
6 medical records.

7 129. As a user navigated to Banner’s page for patients and then to a subpage for medical  
8 records, Banner sent a series of SubscribedButtonClick, PageView, and Microdata events  
9 informing Facebook about those activities. The Microdata events reveal information about the  
10 pages that the user was viewing. For example, the Microdata event associated with the Patient page  
11 reveal that the page the user was viewing offered “resources . . . to make your patient visit or stay  
12 at a Banner Health location as comfortable and successful as possible.”

13 130. Similarly, the Microdata event for the Medical Records page disclose that users  
14 “can request copies of your medical record information” from Banner.

15 131. Moreover, Banner also disclosed information about users’ interactions related to  
16 medical bills. Upon the user clicking a button to open and loading a page about payment options  
17 and other billing information, Banner sent SubscribedButtonClick, PageView, and Microdata  
18 events, disclosing that the user clicked on a button to access Banner’s “patients/billing” page where  
19 they could “Learn more about the financial assistance programs, pricing, insurance information,  
20 programs and policies available for you at Banner Health.”

21 132. From Banner’s Billing page, the user had the option to pay their bill for services  
22 received from Banner’s various service centers: (i) the imaging section, (ii) the surgery center,  
23 (iii) urgent care unit, or (iv) the Wyoming Medical Center.

1           133. As the user clicked to pay their bill for imaging services, surgery center services,  
2 urgent care services, or Wyoming Medical Center services, Banner sent a SubscribedButtonClick  
3 event informing Facebook that the user clicked on a button labeled “Imaging online payment,”  
4 “Surgery Center online payment,” “Urgent Care online payment,” or “Wyoming Medical Center  
5 online payment,” respectively.

6           134. After the pages for the different Banner service centers loaded, Banner also sent a  
7 pair of PageView and Microdata events, each of which revealed additional data about the pages  
8 that the user was viewing. For instance, the Microdata event sent for the surgery center page  
9 informed Facebook that the user was viewing a page that was “Your one-stop shop for all Banner  
10 Surgery Center payment processes.”

11           135. When the user proceeded to pay, for example, on the urgent care billing page,  
12 Banner disclosed that activity as well through a SubscribedButtonClick event.

13           136. Banner also disclosed when the user loaded the login page for Wyoming Medical  
14 Center through a PageView event.

15                           Banner Discloses Users’ Identifying Information

16           137. In addition, as noted, the Meta Pixel collects and transmits to Facebook other  
17 identifying information, including Users’ IP addresses, and users’ “c\_user” cookies, which  
18 Facebook uses to identify users.

19           138. Therefore, the Meta Pixel events Banner sent likely allowed Facebook to connect  
20 users’ identities with the details reported within the events.

21           139. After receiving this information from Defendant, Facebook processes it, analyzes  
22 it, and assimilates it into its own massive datasets, before selling access to this data in the form of  
23 targeted advertisements. Employing “Audiences”—subsections of individuals identified as

1 sharing common traits—Facebook promises the ability to “find the people most likely to respond  
 2 to your ad.”<sup>75</sup> Advertisers can purchase the ability to target their ads based on a variety of criteria:  
 3 “Core Audiences,” individuals who share a location, age, gender, and/or language;<sup>76</sup> “Custom  
 4 Audiences,” individuals who have taken a certain action, such as visiting a website, using an app,  
 5 or buying a product bought a product;<sup>77</sup> and/or “Lookalike Audiences,” groups of individuals who  
 6 “resemble” a Custom Audience, and who, as Facebook promises, “are likely to be interested in  
 7 your business because they’re similar to your best existing customers.”<sup>78</sup>

8 140. Google and other companies process data in a similar manner and use it to build  
 9 marketing and other data profiles allowing for targeted advertising.

10 141. Defendant could have chosen not to use the Meta Pixel, or it could have configured  
 11 it to limit the information that it communicated to third parties, but it did not. Instead, it  
 12 intentionally selected and took advantage of the features and functionality of the Pixel that resulted  
 13 in the Disclosure of Plaintiff’s and Class Members’ Private Information.

14 142. Along those same lines, Defendant could have chosen not to use other tracking  
 15 technologies such as, Google Analytics with Google Tag Manager (“GTM”), Facebook Events,  
 16 AppDynamics, Taboola, Pinterest, StackAdapt, LinkedIn, DoubleClick, Skai, Microsoft Universal  
 17 Events, and Medallia to track Plaintiff and Class Members private communications and transmit  
 18 that information to unauthorized third parties. It did so anyway, intentionally taking advantage of  
 19 these trackers despite the harm to Plaintiff’s and Class Members’ privacy.

21 \_\_\_\_\_  
 22 <sup>75</sup> Audience Ad Targeting, Meta, <https://www.facebook.com/business/ads/ad-targeting> (last  
 visited Aug. 14, 2023).

23 <sup>76</sup> *Id.*

<sup>77</sup> *Id.*

<sup>78</sup> How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Help Center,  
<https://www.facebook.com/business/help/465262276878947> (last visited Aug. 14, 2023).

1           143. Defendant used and disclosed Plaintiff's and Class Members' Private Information  
2 to Facebook, and possibly other third parties, for the purpose of marketing their services and  
3 increasing its profits.

4           144. On information and belief, Defendant shared, traded, or sold Plaintiff's and Class  
5 Members' Private Information with Facebook, and potentially other third parties, in exchange for  
6 improved targeting and marketing services.

7           145. Plaintiff and the Class Members never consented, agreed, authorized, or otherwise  
8 permitted Defendant Banner to intercept their communications or to use or disclose their Private  
9 Information for marketing purposes. Plaintiff and the Class were never provided with any written  
10 notice that Defendant disclosed its patients' Protected Health Information to Facebook and others,  
11 nor were they provided any means of opting out of such disclosures. Defendant nonetheless  
12 knowingly disclosed Plaintiff's and the Class's Protected Health Information to unauthorized  
13 entities.

14           146. Plaintiff and Class Members relied on Defendant to keep their Private Information  
15 confidential and securely maintained, to use this information for legitimate healthcare purposes  
16 only, and to make only authorized disclosures of this information.

17           147. Furthermore, Defendant actively misrepresented that it would preserve the security  
18 and privacy of Plaintiff's and Class Members' Private Information. In actuality, Defendant shared  
19 data about Plaintiff's and Class Members' activities on the Online Platforms alongside identifying  
20 details about the Plaintiff and Class Members, such as their IP addresses.

21           148. By law, Plaintiff and the Class Members are entitled to privacy in their Protected  
22 Health Information and confidential communications. Banner deprived Plaintiff and Class  
23 Members of their privacy rights when it (1) implemented a system that surreptitiously tracked,

1 recorded, and disclosed Plaintiff's and Class Members' confidential communications, Personally  
 2 Identifiable Information, and Protected Health Information; (2) disclosed patients' Private  
 3 Information to unauthorized, third-party eavesdroppers, including Facebook and possibly others;  
 4 and (3) undertook this pattern of conduct without notifying Plaintiff and Class Members and  
 5 without obtaining their express written consent.

#### 6 **B. Plaintiff's Experience**

7 149. Plaintiff has been a patient of Defendant since 2008, approximately, receiving  
 8 healthcare services from Banner and physicians in Banner's network, including for spinal  
 9 degeneration at Banner Lassen Medical Center in Susanville, California.

10 150. Plaintiff relied on Banner's Website and Online Platforms to communicate  
 11 confidential patient information, beginning in 2021 using personal computing devices in Lassen  
 12 County, and last in October 2023. Specifically, he used the Website's search function to search  
 13 for health information on spinal degeneration, and to search for physicians;<sup>79</sup> used the Website's  
 14 find a doctor function;<sup>80</sup> used the patient account and/or patient portal, including to make medical  
 15 appointments, check laboratory results, and make recurring payments of bills for services.<sup>81</sup>

16 151. Plaintiff accessed Defendant's Website and Online Platforms at Defendant's  
 17 direction and encouragement. Plaintiff reasonably expected that his communications with Banner  
 18 were confidential, solely between himself and Banner, and that, as such, those communications  
 19 would not be transmitted to or intercepted by a third party.

20 152. Plaintiff provided his Private Information to Defendant and trusted that the  
 21

---

22 <sup>79</sup> E.g., search for "chest pain," avail. at  
<https://www.bannerhealth.com/search?query=chest%20pain> (last acc. Mar. 8, 2024).

23 <sup>80</sup> <https://www.bannerhealth.com/physician-directory> (last acc. Mar. 8, 2024).

<sup>81</sup> [https://account.bannerhealth.com/sign-in?\\_ga=2.66854765.237380448.1709911311-131706459.1709911311](https://account.bannerhealth.com/sign-in?_ga=2.66854765.237380448.1709911311-131706459.1709911311) (last acc. Mar. 8, 2024).



1 information would be safeguarded according to Banner's Privacy Policies and the law.

2 153. On information and belief, through its use of the Meta Pixel on the Website and  
3 Online Platforms, Defendant disclosed to Facebook:

- 4 a. Plaintiff's identity via his IP addresses and/or "c\_user" cookies;
- 5 b. Plaintiff's seeking of medical treatment;
- 6 c. Plaintiff's status as a patient;
- 7 d. Plaintiff's search terms and activities, including relating to his health  
8 information and diagnoses, and doctors;
- 9 e. The doctors Plaintiff searched for and viewed;
- 10 f. The pages and content Plaintiff viewed; and,
- 11 g. Plaintiff's activity on the patient account and/or patient portal, including the  
12 appointments he scheduled, his laboratory results, and bills he paid.

13 154. By failing to receive the requisite consent, Banner breached confidentiality and  
14 unlawfully disclosed Plaintiff's Private Information.

15 155. Plaintiff first discovered that Defendant was using the Meta Pixel and other tracking  
16 technologies to gather and disclose his Private Information in October of 2023.

17 156. As a result of Banner's Disclosure of Plaintiff's Private Information via the Meta  
18 Pixel and other tracking technologies to third parties without authorization, Plaintiff now receives  
19 targeted health-related advertisements relating to spinal degeneration and having a newborn baby,  
20 reflecting his private medical treatment information.

21 157. Plaintiff paid Banner for medical services and the services he paid for included  
22 reasonable privacy and data security protections for his Private Information, but Plaintiff did not  
23 receive the privacy and security protections for which he paid, due to Defendant's Disclosure.

1           158. Because of Defendant's unauthorized Disclosure of his Private Information,  
2 Plaintiff has suffered injuries, including monetary damages; loss of privacy; unauthorized  
3 disclosure of this Private Information; unauthorized access to his Private Information by third  
4 parties; use of the Private Information for advertising purposes; embarrassment, humiliation,  
5 frustration, and emotional distress; decreased value of his Private Information; lost benefit of the  
6 bargain; and increased risk of future harm resulting from further unauthorized use and disclosure  
7 of his information.

8           **C. Investigations and Reports Reveal the Meta Pixel's Impermissible Collection of PHI**

9           159. In June 2020, after promising users that app developers would not have access to  
10 data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party  
11 developers to access this data.<sup>82</sup> This failure to protect users' data enabled thousands of developers  
12 to see data on inactive users' accounts if those users were Facebook friends with someone who  
13 was an active user.

14           160. On February 18, 2021, the New York State Department of Financial Services  
15 released a report detailing the significant privacy concerns associated with Facebook's data  
16 collection practices, including the collection of health data. The report noted that while Facebook  
17 maintained a policy that instructed developers not to transmit sensitive medical information,  
18 Facebook received, stored, and analyzed this information anyway. The report concluded that  
19 "[t]he information provided by Facebook has made it clear that Facebook's internal controls on  
20 this issue have been very limited and were not effective . . . at preventing the receipt of sensitive  
21  
22  
23

---

<sup>82</sup> Kurt Wagner & Bloomberg, Facebook Admits Another Blunder with User Data, FORTUNE (July 1, 2020 at 6:30 p.m.) <https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/>.

1 data.”<sup>83</sup>

2 161. The New York State Department of Financial Service’s concern about Facebook’s  
3 cavalier treatment of private medical data was not misplaced. In June 2022, the FTC finalized a  
4 different settlement involving Facebook’s monetizing of sensitive medical data. In that case, the  
5 more than 100 million users of Flo, a period and ovulation tracking app, learned something  
6 startling: the company was sharing their data with Facebook.<sup>84</sup> When a user was having his period  
7 or informed the app of his intention to get pregnant, Flo would tell Facebook, which could then  
8 use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the  
9 Federal Trade Commission for lying to its users about secretly sharing their data with Facebook,  
10 as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and  
11 Flurry. The FTC reported that Flo “took no action to limit what these companies could do with  
12 users’ information.”<sup>85</sup>

13 162. More recently, Facebook employees admitted to lax protections for sensitive user  
14 data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that  
15 “[w]e do not have an adequate level of control and explainability over how our systems use data,  
16 and thus we can’t confidently make controlled policy changes or external commitments such as  
17 ‘we will not use X data for Y purpose.’”<sup>86</sup>

18  
19  
20 <sup>83</sup> New York State Department of Financial Services, REPORT ON INVESTIGATION OF FACEBOOK  
INC. DATA PRIVACY CONCERNS, (Feb. 18, 2021)

[https://www.dfs.ny.gov/system/files/documents/2021/02/facebook\\_report\\_20210218.pdf](https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf).

21 <sup>84</sup> Justin Sherman, Your Health Data Might Be for Sale, SLATE (June 22, 2022 at 5:50 a.m.)  
22 <https://slate.com/technology/2022/06/health-data-brokers-privacy.html>.

<sup>85</sup> *Id.*

23 <sup>86</sup> Lorenzo Franceschi-Bicchierai, Facebook Doesn’t Know What It Does with Your Data, or  
Where It Goes: Leaked Document, VICE (April 26, 2022)

<https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes>.

1 163. Furthermore, in June 2022, an investigation by The Markup<sup>87</sup> revealed that the Meta  
 2 Pixel was embedded on the websites of 33 of the top 100 hospitals in the nation.<sup>88</sup> On those hospital  
 3 websites, the Meta Pixel collects and sends Facebook a “packet of data,” including sensitive  
 4 personal health information, whenever a user interacts with the website, for example, by clicking  
 5 a button to schedule a doctor’s appointment.<sup>89</sup> The data is connected to an IP address, which is “an  
 6 identifier that’s like a computer’s mailing address and can generally be linked to a specific  
 7 individual or household—creating an intimate receipt of the appointment request for Facebook.”<sup>90</sup>

8 164. During its investigation, The Markup found that Facebook’s purported “filtering”  
 9 failed to discard even the most obvious forms of sexual health information. Worse, the article  
 10 found that the data that the Meta Pixel was sending Facebook from hospital websites not only  
 11 included details such as patients’ medications, descriptions of their allergic reactions, details about  
 12 their upcoming doctor’s appointments, but also included patients’ names, addresses, email  
 13 addresses, and phone numbers.<sup>91</sup>

14 165. In addition to the 33 hospitals identified by The Markup that had installed the Meta  
 15 Pixel on their websites, The Markup identified seven health systems that had installed the Meta  
 16 Pixel inside their password-protected patient portals.<sup>92</sup>

17 166. David Holtzman, health privacy consultant and former senior privacy adviser in the  
 18

19 \_\_\_\_\_  
 20 <sup>87</sup> The Markup is a nonprofit newsroom that investigates how powerful institutions are using  
 technology to change our society. *See* [www.themarkup.org/about](http://www.themarkup.org/about) (last accessed Mar. 19, 2023).

21 <sup>88</sup> Todd Feathers, Simon Fondrie-Teitler, Angie Waller, & Surya Mattu, Facebook Is Receiving  
 Sensitive Medical Information from Hospital Websites, THE MARKUP (June 16, 2022 6:00 a.m.)  
 22 [https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-](https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites)  
 information-from-hospital-websites.

23 <sup>89</sup> *Id.*

<sup>90</sup> *Id.*

<sup>91</sup> *Id.*

<sup>92</sup> *Id.*

1 U.S. Department of Health and Human Services' Office for Civil Rights, stated he was "deeply  
2 troubled" by what the hospitals capturing and sharing patient data in this way.<sup>93</sup>

3 **D. Defendant Violated HIPAA Standards**

4 167. Under HIPAA, a healthcare provider may not disclose personally identifiable, non-  
5 public medical information (PHI) about a patient, a potential patient, or household member of a  
6 patient for marketing purposes without the patients' express written authorization.<sup>94</sup>

7 168. Guidance from the United States Department of Health and Human Services  
8 instructs healthcare providers that patient status alone is protected by HIPAA.

9 169. In Guidance regarding Methods for De-identification of Protected Health  
10 Information in Accordance with the Health Insurance Portability and Accountability Act Privacy  
11 Rule, the Department instructs:

12 Identifying information alone, such as personal names, residential addresses, or  
13 phone numbers, would not necessarily be designated as PHI. For instance, if such  
14 information was reported as part of a publicly accessible data source, such as a  
15 phone book, then this information would not be PHI because it is not related to  
16 health data... If such information was listed with health condition, health care  
17 provision, or payment data, such as an indication that the individual was treated at  
18 a certain clinic, then this information would be PHI.<sup>95</sup>

16 170. In its guidance for Marketing, the Department further instructs:

17 The HIPAA Privacy Rule gives individuals important controls over whether and  
18 how their protected health information is used and disclosed for marketing  
19 purposes. With limited exceptions, the Rule requires an individual's written  
20 authorization before a use or disclosure of his or his protected health information  
21 can be made for marketing. ... Simply put, a covered entity may not sell protected  
22 health information to a business associate or any other third party for that party's

---

21 <sup>93</sup> *Id.*

22 <sup>94</sup> HIPAA, 42 U.S.C. § 1320; 45 C.F.R. §§ 164.502; 164.508(a)(3), 164.514(b)(2)(i).

23 <sup>95</sup> U.S. Department of Health and Human Services, Guidance Regarding Methods for De-  
identification of Protected Health Information in Accordance with the Health Insurance  
Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012)  
[https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/De-  
identification/hhs\\_deid\\_guidance.pdf](https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveridentities/De-identification/hhs_deid_guidance.pdf).

own purposes. Moreover, covered entities may not sell lists of patients to third parties without obtaining authorization from each person on the list. (Emphasis added).<sup>96</sup>

171. In addition, the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) has issued a Bulletin to highlight the obligations of HIPAA-covered entities and business associates (“regulated entities”) under the HIPAA Privacy, Security, and Breach Notification Rules (“HIPAA Rules”) when using online tracking technology.<sup>97</sup>

172. According to the Bulletin, “HIPAA Rules apply when the information that regulated entities collect through tracking technologies or disclose to tracking technology vendors includes protected health information.”<sup>98</sup>

173. Citing The Markup’s June 2022 article, the Bulletin expressly notes:

Some regulated entities may share sensitive information with online tracking technology vendors and such sharing may be unauthorized disclosures of PHI with such vendors. **Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.** For example, disclosures of PHI to tracking technology vendors or marketing purposes, without individuals’ HIPAA-compliant authorizations, would constitute impermissible disclosures.

An impermissible disclosure of an individual’s PHI not only violates the Privacy Rule but also may result in a wide range of additional harms to the individual or others. For example, an impermissible disclosure of PHI may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to others identified in the individual’s PHI. Such disclosures can reveal incredibly sensitive information about an individual, including diagnoses, frequency of visits to a therapist or other health care professionals, and where an individual seeks medical treatment. While it has always been true that regulated entities may not

<sup>96</sup> U.S. Department of Health and Human Services, Marketing, (Dec. 3, 2002) <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf>.

<sup>97</sup> See U.S. Department of Health and Human Services, Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, <https://www.hhs.gov/hipaa/forprofessionals/privacy/guidance/hipaa-online-tracking/index.html>.

<sup>98</sup> *Id.*

1 impermissibly disclose PHI to tracking technology vendors, because of the  
 2 proliferation of tracking technologies collecting sensitive information, now more  
 3 than ever, it is critical for regulated entities to ensure that they disclose PHI **only** as  
 4 expressly permitted or required by the HIPAA Privacy Rule.<sup>99</sup>

5 174. In other words, HHS has expressly stated that Defendant's conduct of  
 6 implementing the Meta Pixel is a violation of HIPAA Rules.

7 **E. Defendant Violated FTC Standards, and the FTC and HHS Take Action**

8 175. The Federal Trade Commission ("FTC") has also recognized that implementation  
 9 of the Meta Pixel and other tracking technologies pose "serious privacy and security risks" and  
 10 "impermissibly disclos[e] consumers' sensitive personal health information to third parties."<sup>100</sup>

11 176. On July 20, 2023, the FTC and HHS sent a "joint letter to approximately 130  
 12 hospital systems and telehealth providers to alert them about the risks and concerns about the use  
 13 of technologies, such as Meta/Facebook pixel and Google Analytics, that can track a user's online  
 14 activities."<sup>101</sup>

15 177. Therein, the FTC reminded healthcare providers that "HIPAA regulated entities are  
 16 not permitted to use tracking technologies in a manner that would result in impermissible  
 17 disclosures of PHI to third parties or any other violations of the HIPAA Rules"<sup>102</sup> and that "[t]his  
 18 is true even if you relied upon a third party to develop your website or mobile app and even if you  
 19 do not use the information obtained through use of a tracking technology for any marketing

20 <sup>99</sup> *Id.* (emphasis in original) (internal citations omitted).

21 <sup>100</sup> Re: Use of Online Tracking Technologies, U.S. Dep't of Health & Human Services, (July 20,  
 22 2023) (available at [https://www.ftc.gov/system/files/ftc\\_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/FTC-OCR-Letter-Third-Party-Trackers-07-20-2023.pdf)), **Exhibit A**.

23 <sup>101</sup> FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security  
 Risks from Online Tracking Technologies, FEDERAL TRADE COMMISSION (July 20, 2023)  
[https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm\\_source=govdelivery](https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking?utm_source=govdelivery).

<sup>102</sup> *Id.*



1 purposes.”<sup>103</sup>

2 178. Entities that are not covered by HIPAA also face accountability for disclosing  
 3 consumers’ sensitive health information under the Health Breach Notification Rule. 16 C.F.R. §  
 4 318. This Rule requires that companies dealing with health records notify the FTC and consumers  
 5 if there has been a breach of unsecured identifiable health information, or else face civil penalties  
 6 for violations. *Id.* According to the FTC, “a ‘breach’ is not limited to cybersecurity intrusions or  
 7 nefarious behavior. Incidents of unauthorized access, *including sharing of covered information*  
 8 *without an individual’s authorization*, triggers notification obligations under the Rule.”<sup>104</sup>

9 179. Additionally, the FTC Act makes it unlawful to employ “[u]nfair methods of  
 10 competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting  
 11 commerce[.]” 15 U.S.C. § 45(a). According to the FTC, “the disclosure of [sensitive health]  
 12 information without a consumer’s authorization can, in some circumstances, violate the FTC Act  
 13 as well as constitute a breach of security under the FTC’s Health Breach Notification Rule.”<sup>105</sup>

14 180. As such, the FTC and HHS have expressly stated that conduct like Defendant’s  
 15 runs afoul of the FTC Act and/or the FTC’s Health Breach Notification Rule.

---

18 <sup>103</sup> *Id.*

19 <sup>104</sup> Statement of the Commission: On Breaches by Health Apps and Other Connected Devices,  
 U.S. Fed. Trade Commission, (Sept. 15, 2021) (available at  
 20 [https://www.ftc.gov/system/files/documents/public\\_statements/1596364/statement\\_of\\_the\\_commission\\_on\\_breaches\\_by\\_health\\_apps\\_and\\_other\\_connected\\_devices.pdf](https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf)) (emphasis added).

21 <sup>105</sup> See, e.g., U.S. v. Easy Healthcare Corp., Case No. 1:23-cv-3107 (N.D. Ill. 2023),  
<https://www.ftc.gov/legallibrary/browse/cases-proceedings/202-3186-easy-healthcare-corporation-us-v>;  
 22 In the Matter of BetterHelp, Inc., FTC Dkt. No. C-4796 (July 14, 2023),  
<https://www.ftc.gov/legal-library/browse/cases-proceedings/2023169-betterhelp-inc-matter>; U.S.  
 23 v. GoodRx Holdings, Inc., Case No. 23-cv-460 (N.D. Cal. 2023), <https://www.ftc.gov/legal-library/browse/cases-proceedings/2023090-goodrx-holdings-inc>; In the Matter of Flo Health Inc., FTC Dkt. No. C-4747 (June 22, 2021), <https://www.ftc.gov/legal-library/browse/casesproceedings/192-3133-flo-health-inc>.

**F. Defendant Violated Industry Standards**

181. A medical provider's duty of confidentiality is a cardinal rule and is embedded in the physician-patient and hospital-patient relationship.

182. The American Medical Association's ("AMA") Code of Medical Ethics contains numerous rules protecting the privacy of patient data and communications, which are applicable to Banner and its physicians.

183. AMA Code of Ethics Opinion 3.1.1 provides:

Protecting information gathered in association with the care of the patient is a core value in health care . . . . Patient privacy encompasses a number of aspects, including . . . personal data (informational privacy).

184. AMA Code of Medical Ethics Opinion 3.2.4 provides:

Information gathered and recorded in association with the care of the patient is confidential. Patients are entitled to expect that the sensitive personal information they divulge will be used solely to enable their physician to most effectively provide needed services. Disclosing information for commercial purposes without consent undermines trust, violates principles of informed consent and confidentiality, and may harm the integrity of the patient-physician relationship. Physicians who propose to permit third-party access to specific patient information for commercial purposes should: (a) Only provide data that has been de-identified. [and] (b) Fully inform each patient whose record would be involved (or the patient's authorized surrogate when the individual lacks decision-making capacity about the purposes for which access would be granted.

185. AMA Code of Medical Ethics Opinion 3.3.2 provides:

Information gathered and recorded in association with the care of a patient is confidential, regardless of the form in which it is collected or stored. Physicians who collect or store patient information electronically . . . must . . . release patient information only in keeping ethics guidelines for confidentiality.

**G. Plaintiff's and Class Members' Expectation of Privacy**

186. At all times when Plaintiff and Class Members provided their Private Information to Defendant, they all had a reasonable expectation that the information would remain private and that Defendant would not share the Private Information with third parties for a commercial

1 marketing and sales purposes, unrelated to patient care.

2 **H. IP Addresses are Personally Identifiable Information**

3 187. Defendant also disclosed and otherwise assisted Facebook and potentially others  
4 with intercepting Plaintiff's and Class Members' IP addresses using the Meta Pixel and other  
5 tracking technologies.

6 188. An IP address is a number that identifies the address of a device connected to the  
7 Internet.

8 189. IP addresses are used to identify and route communications on the Internet.

9 190. IP addresses of individual Internet users are used by Internet service providers,  
10 Websites, and third-party tracking companies to facilitate and track Internet communications.

11 191. Facebook tracks every IP address ever associated with a Facebook user.

12 192. Facebook tracks IP addresses for use of targeting individual homes and their  
13 occupants with advertising.

14 193. Under HIPAA, an IP address is Personally Identifiable Information:

- 15 • HIPAA defines personally identifiable information to include "any unique  
16 identifying number, characteristic or code" and specifically lists the example of IP  
addresses. *See* 45 C.F.R. § 164.514 (2).
- 17 • HIPAA further declares information as personally identifiable where the covered  
18 entity has "actual knowledge that the information to identify an individual who is a  
subject of the information." 45 C.F.R. § 164.514(2)(ii); *See also*, 45 C.F.R. §  
164.514(b)(2)(i)(O).

19 194. Consequently, by disclosing IP addresses, Defendant's business practices violated  
20 HIPAA and industry privacy standards.  
21  
22  
23

**I. Defendant Was Enriched and Benefitted from the Use of The Pixel and Unauthorized Disclosures**

195. The sole purpose for Defendant's use of the Meta Pixel and other tracking technology was marketing and profits.

196. In exchange for disclosing the Private Information of its patients, Defendant is compensated by Facebook and likely others in the form of enhanced advertising services and more cost-efficient marketing on its platform.

197. Retargeting is a form of online marketing that targets users with ads based on their previous internet communications and interactions. Upon information and belief, as part of its marketing campaign, Defendant re-targeted patients and potential patients.

198. By utilizing the Meta Pixel and other trackers, the cost of advertising and retargeting was reduced, thereby benefiting Defendant.

**J. Plaintiff's and Class Members' Private Information Had Financial Value**

199. The data concerning Plaintiff and Class Members, collected and shared by Defendant, has tremendous economic value. Data collected via the Meta Pixel, CAPI, and other online tracking tools allows Facebook to build its own massive, proprietary dataset, to which it then sells access in the form of targeted advertisements. Targeting works by allowing advertisers to direct their ads at particular "Audiences," subsets of individuals who, according to Facebook, are the "people most likely to respond to your ad."<sup>106</sup> Facebook's "Core Audiences" allow advertisers to target individuals based on demographics, such as age, location, gender, or language, whereas "Custom Audiences" allow advertisers to target individuals who have "already shown interest in your business," by visiting a business's website, using an app, or engaging in certain

---

<sup>106</sup> Audience Ad Targeting, Meta, <https://www.facebook.com/business/ads/ad-targeting> (last visited Aug. 14, 2023).

1 online content.<sup>107</sup> Facebook’s “Lookalike Audiences” go further, targeting individuals who  
2 resemble current customer profiles and whom, according to Facebook, “are likely to be interested  
3 in your business.”<sup>108</sup>

4 200. Data harvesting is big business, and it drives Facebook’s profit center, its  
5 advertising sales. In 2019, Facebook generated nearly \$70 billion dollars in advertising revenue  
6 alone, constituting more than 98% of its total revenue for that year.<sup>109</sup>

7 201. This business model is not limited to Facebook. Data harvesting one of the fastest  
8 growing industries in the country, and consumer data is so valuable that it has been described as  
9 the “new oil.” Conservative estimates suggest that in 2018, Internet companies earned \$202 per  
10 American user from mining and selling data. That figure is only due to keep increasing; estimates  
11 for 2022 were as high as \$434 per user, for a total of more than \$200 billion industry wide.

12 202. In particular, the value of health data is well-known due to the media’s extensive  
13 reporting on the subject. For example, Time Magazine published an article in 2017 titled “How  
14 Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry.” Therein, Time Magazine  
15 described the extensive market for health data and observed that the health data market is both  
16 lucrative and a significant risk to privacy.<sup>110</sup>

17 203. Similarly, CNBC published an article in 2019 in which it observed that “[d]e-  
18 identified patient data has become its own small economy: There’s a whole market of brokers who  
19

---

20 <sup>107</sup> *Id.*

21 <sup>108</sup> See How to Create a Lookalike Audience on Meta Ads Manager, Meta Business Center,  
<https://www.facebook.com/business/help/465262276878947> (last visited Aug. 14, 2023).

22 <sup>109</sup> See Here’s How Big Facebook’s Ad Business Really Is, CNN,  
<https://www.cnn.com/2020/06/30/tech/facebook-ad-business-boycott/index.html> (last visited  
23 Aug. 14, 2023).

<sup>110</sup> See Adam Tanner, How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry,  
TIME, (Jan. 9, 2017 at 9:00 a.m.) <https://time.com/4588104/medical-data-industry/>.

1 compile the data from providers and other health-care organizations and sell it to buyers.”<sup>111</sup>

2 **TOLLING, CONCEALMENT, AND ESTOPPEL**

3 204. The applicable statutes of limitation have been tolled as a result of Banner’s  
4 knowing and active concealment and denial of the facts alleged herein.

5 205. Banner seamlessly incorporated Meta Pixel and other trackers into its Website and  
6 Online Platforms while providing users with no indication that their Website usage was being  
7 tracked and transmitted to third parties. Banner knew that its Website incorporated Meta Pixel and  
8 other trackers, yet it failed to disclose to Plaintiff and Class Members that their sensitive medical  
9 information would be intercepted, collected, used by, and disclosed to Facebook and likely other  
10 third parties.

11 206. Plaintiff and Class Members could not with due diligence have discovered the full  
12 scope of Banner’s conduct, because there were no disclosures or other indication that they were  
13 interacting with websites employing Meta Pixel or any other tracking technology.

14 207. All applicable statutes of limitation have also been tolled by operation of the  
15 discovery rule and the doctrine of continuing tort. Banner’s illegal interception and disclosure of  
16 Plaintiff’s Private Information has continued unabated. What is more, Banner was under a duty to  
17 disclose the nature and significance of its data collection practices but did not do so. Banner is  
18 therefore estopped from relying on any statute of limitations defenses.

19  
20  
21  
22  
23 <sup>111</sup> See Christina Farr, Hospital Execs Say They are Getting Flooded with Requests for Your Health Data, CNBC, (Dec. 18, 2019 at 8:27 a.m.) <https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html>.

CLASS ALLEGATIONS

208. Plaintiff brings this nationwide class action individually, and on behalf of all other similarly situated persons, pursuant to Cal. Civ. P. § 382.

209. The nationwide Class that Plaintiff seeks to represent is defined as follows:

**All persons whose Private Information was disclosed by Defendant to third parties through the Meta Pixel and related technology without authorization.**

210. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels, and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

211. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

212. Numerosity: Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are hundreds or thousands of individuals whose Private Information may have been improperly used or disclosed by Defendant, and the Class is identifiable within Defendant's records.

213. Commonality: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class Members. These include:

- a. whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' Private Information;
- b. whether Defendant had duties not to disclose the Plaintiff's and Class



Members' Private Information to unauthorized third parties;

c. whether Defendant had duties not to use Plaintiff's and Class Members'

Private Information for non-healthcare purposes;

d. whether Defendant had duties not to use Plaintiff's and Class Members'

Private Information for unauthorized purposes;

e. whether Defendant failed to adequately Plaintiff's and Class Members'

Private Information;

f. whether Defendant adequately, promptly, and accurately informed Plaintiff

and Class Members that their Private Information had been compromised;

g. whether Defendant violated the law by failing to promptly notify Plaintiff

and Class Members that their Private Information had been compromised;

h. whether Defendant failed to properly implement and configure the tracking

software on its Online Platforms to prevent the disclosure of confidential

communications and Private Information;

i. whether Defendant committed invasion of privacy;

j. whether Defendant breached its implied contracts with Plaintiff and the

Class Members;

k. or in the alternate, whether Defendant was unjustly enriched;

l. whether Defendant breached fiduciary duties to Plaintiff and the Class

Members;

m. whether Defendant violated the California Invasion of Privacy Act

("CIPA"), Cal. Penal Code §§ 630, *et seq.*;

n. whether Defendant violated the California Confidentiality of Medical

Information Act (“CMIA”), Cal. Civil Code §§ 56.06, 56.10, and 56.101;

o. whether Defendant violated the Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal. Penal Code § 502;

p. whether Defendant engaged in unfair, unlawful, or deceptive practices in violation of Cal. Bus. & Prof. Code §§ 17200, *et. seq.*; and,

q. whether Plaintiff and the Class Members are entitled to monetary damages, including compensatory and statutory damages, and the sums thereof.

214. Typicality: Plaintiff’s claims are typical of those of other Class Members because all had their Private Information compromised as a result of Defendant’s use and incorporation of Meta Pixel and other tracking technology.

215. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court’s imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant’s policies challenged herein apply to and affect Class Members uniformly, and Plaintiff’s challenge of these policies hinges on Defendant’s conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

216. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages Plaintiff has suffered is typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

217. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

218. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged. If the class action device were not used, Defendant would necessarily gain an unconscionable advantage because they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources. Moreover, the costs of individual suits could unreasonably consume the amounts that would be recovered, whereas proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged. Finally, individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

219. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

1 Members demonstrates that there would be no significant manageability problems with  
2 prosecuting this lawsuit as a class action.

3 220. Adequate notice can be given to Class Members directly using information  
4 maintained in Defendant's records.

5 221. Unless a Class-wide injunction is issued, Defendant may continue in its unlawful  
6 use and disclosure and failure to properly secure the Private Information of Class Members,  
7 Defendant may continue to refuse to provide proper notification to and obtain proper consent from  
8 Class Member, and Defendant may continue to act unlawfully as set forth in this Complaint.

9 222. Further, Defendant has acted or refused to act on grounds generally applicable to  
10 the Class, and, accordingly, final injunctive or corresponding declaratory relief regarding the  
11 whole of the Class is appropriate.

12 223. Likewise, particular issues are appropriate for certification because such claims  
13 present only particular, common issues, the resolution of which would advance the disposition of  
14 this matter and the parties' interests therein. Such particular issues include, but are not limited to  
15 the following:

- 16 a. whether Defendant owed a legal duty to Plaintiff and Class Members to  
17 exercise due care in collecting, storing, using, and safeguarding their Private  
18 Information;
- 19 b. whether Defendant breached a legal duty to Plaintiff and Class Members to  
20 exercise due care in collecting, storing, using, and safeguarding their Private  
21 Information;
- 22 c. whether Defendant failed to comply with its own policies and applicable  
23 laws, regulations, and industry standards relating to the disclosure of patient

information;

d. whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. whether Defendant breached the implied contract;

f. in the alternate, whether Defendant was unjustly enriched;

g. whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been used and disclosed to third parties;

h. whether Defendant failed to implement and maintain reasonable security procedures and practices;

i. whether Defendant committed an invasion of privacy;

j. whether Defendant had fiduciary duties to Plaintiff and the Class Members;

k. whether Defendant breached its fiduciary duties;

l. whether Defendant violated the California Invasion of Privacy Act (“CIPA”), Cal. Penal Code §§ 630, *et seq.*;

m. whether Defendant violated the California Confidentiality of Medical Information Act (“CMIA”), Cal. Civil Code §§ 56.06, 56.10, and 56.101;

n. whether Defendant violated the Comprehensive Computer Data Access and Fraud Act (“CDAFA”), Cal. Penal Code § 502;

o. whether Defendant engaged in unfair, unlawful, or deceptive practices in violation of Cal. Bus. & Prof. Code §§ 17200, *et seq.*; and,

p. whether Plaintiff and the Class Members are entitled to actual,

consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

**COUNT I**  
**NEGLIGENCE**  
**(On Behalf of Plaintiff and the Class)**

224. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

225. Defendant owed to Plaintiff and Class Members a duty to exercise reasonable care in handling and using Plaintiff's and Class Members' Private Information in its care and custody, including implementing industry-standard privacy procedures sufficient to reasonably protect the information from the disclosure and unauthorized transmittal and use of Private Information that occurred.

226. Defendant acted with wanton and reckless disregard for the privacy and confidentiality of Plaintiff's and Class Members' Private Information by disclosing and providing access to this information to third parties for the financial benefit of the third parties and Defendant.

227. Defendant owed these duties to Plaintiff and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's Disclosure of their Private Information to benefit third parties and Defendant. Defendant actively sought and obtained Plaintiff's and Class Members' Private Information.

228. Private Information is highly valuable, and Defendant knew, or should have known, the harm that would be inflicted on Plaintiff and Class Members by disclosing their Private Information to third parties. This disclosure was of benefit to third parties and Defendant by way of data harvesting, advertising, and increased sales.

229. Defendant breached its common law duties by failing to exercise reasonable care

1 in the handling and securing of Private Information of Plaintiff and Class Members and in the  
2 supervising its agents, contractors, vendors, and suppliers in the handling and securing of Private  
3 Information of Plaintiff and Class Members. This failure actually and proximately caused  
4 Plaintiff's and Class Members' injuries.

5 230. In addition, the standards of care owed by Defendant are established by statute,  
6 including the FTC Act, HIPAA, the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160  
7 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health  
8 Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected  
9 Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C and the other sections  
10 identified above, under which Defendant were required by law to maintain adequate and  
11 reasonable data and cybersecurity measures to maintain the security and privacy of Plaintiff's and  
12 Class Members' Private Information.

13 231. Plaintiff and Class Members are within the class of persons that these statutes and  
14 rules were designed to protect.

15 232. Defendant had a duty to have procedures in place to detect and prevent the loss or  
16 unauthorized dissemination of Plaintiff's and Class Members' Private Information, PII and PHI.

17 233. Defendant owed a duty to timely and adequately inform Plaintiff and Class  
18 Members, in the event of their Private Information, PII and PHI, being improperly disclosed to  
19 unauthorized third parties.

20 234. It was not only reasonably foreseeable, but it was intended, that the failure to  
21 reasonably protect and secure Plaintiff's and Class Members' Private Information, PII and PHI, in  
22 compliance with applicable laws would result in an unauthorized third-parties such as Facebook,  
23 and others gaining access to Plaintiff's and Class Members' PII and PHI, and resulting in



1 Defendant's liability under principles of negligence and negligence *per se*.

2 235. Defendant violated the standards of care under Section 5 of the FTC Act and under  
3 HIPAA and attendant regulations by failing to use reasonable measures to protect Plaintiff's and  
4 Class Members' PII and PHI and not complying with applicable industry standards as described  
5 in detail herein.

6 236. As a direct and traceable result of Defendant's negligence and/or negligent  
7 supervision, and/or negligence *per se*, Plaintiff and Class Members have suffered or will suffer  
8 damages, including monetary damages, inappropriate advertisements, and use of their Private  
9 Information for advertising purposes, and increased risk of future harm, embarrassment,  
10 humiliation, frustration, and emotional distress.

11 237. Plaintiff's and Class Member's PII and PHI constitute personal property that was  
12 taken and misused as a proximate result of Defendant's negligence, resulting in harm, injury, and  
13 damages to Plaintiff and Class Members.

14 238. Defendant's breach of its common-law duties to exercise reasonable care and  
15 negligence directly and proximately caused Plaintiff's and Class Members' actual, tangible, injury-  
16 in-fact and damages, including, without limitation, the unauthorized access of their Private  
17 Information by third parties, improper disclosure of their Private Information, lost benefit of their  
18 bargain, lost value of their Private Information and diminution in value, emotional distress, and  
19 lost time and money incurred to mitigate and remediate the effects of use of their information that  
20 resulted from and were caused by Defendant's negligence. These injuries are ongoing, imminent,  
21 immediate, and continuing.

22 239. In failing to secure Plaintiff's and Class Members' Private Information, PII and  
23 PHI, Defendant are guilty of oppression, fraud, or malice. Defendant acted or failed to act with a

1 reckless, willful, or conscious disregard of Plaintiff and Class Members' rights. Plaintiff, in  
2 addition to seeking actual damages, also seek punitive damages on behalf of themselves and the  
3 Class.

4 240. Defendant's negligence directly and proximately caused the unauthorized access  
5 and Disclosure of Plaintiff's and Class Members' Private Information, PII and PHI, and as a result,  
6 Plaintiff and Class Members have suffered and will continue to suffer damages as a result of  
7 Defendant's conduct. Plaintiff and Class Members seek actual, compensatory, and punitive  
8 damages, and all other relief they may be entitled to as a proximate result of Defendant's  
9 negligence and negligence *per se*.

10 **COUNT II**  
11 **BREACH OF IMPLIED CONTRACT**  
**(On behalf of Plaintiff and the Class)**

12 241. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

13 242. As a condition of receiving medical care from Defendant, Plaintiff and the Class  
14 provided their Private Information and paid monies for medical treatment received. In so doing,  
15 Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant  
16 agreed to safeguard and protect such information, as set forth in its Privacy Policies, and elsewhere,  
17 to keep such information secure and confidential.

18 243. Implicit in the agreement between Defendant and its patients, Plaintiff and the  
19 proposed Class Members, was the obligation that all parties would maintain the Private  
20 Information confidentially and securely.

21 244. Defendant had an implied duty of good faith to ensure that the Private Information  
22 of Plaintiff and Class Members in its possession was only used only as authorized, such as to  
23 provide medical treatment, billing, and other medical benefits from Defendant.

1           245. Defendant had an implied duty to protect the Private Information of Plaintiff and  
2 Class Members from unauthorized disclosure or uses.

3           246. Additionally, Defendant explicitly promised to keep its patients' Private  
4 Information secure and confidential, stating in its Notice of Privacy Practices that, "[o]ther uses  
5 and disclosures not described in this notice will be made only with your written  
6 authorization, such as sale of medical information.." <sup>112</sup>

7           247. Plaintiff and Class Members fully performed their obligations under the implied  
8 contracts with Defendant, but Banner did not. Plaintiff and Class Members would not have  
9 provided their confidential Private Information to Defendant in the absence of their implied  
10 contracts with Defendant that their Private Information would be kept in confidence and would  
11 instead have retained the opportunity to control their Private Information for uses other than  
12 receiving medical treatment from Defendant.

13           248. Defendant breached the implied contracts with Plaintiff and Class members by  
14 disclosing Plaintiff's and Class Members' Private Information to unauthorized third parties.

15           249. Defendant's acts and omissions have materially affected the intended purpose of  
16 the implied contracts that required Plaintiff and Class Members to provide their Private  
17 Information in exchange for medical treatment and benefits.

18           250. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff  
19 and the Class have suffered (and will continue to suffer) actual, tangible, injury-in-fact and  
20 damages, including, without limitation, the unauthorized access of their Private Information by  
21 third parties, improper disclosure of their Private Information, lost benefit of their bargain, lost  
22 value of their Private Information and diminution in value, emotional distress, and lost time and  
23

---

<sup>112</sup> *Notice of Privacy Practices*, **Exhibit B** (bold emphasis added).

1 money incurred to mitigate and remediate the effects of use of their information that resulted from  
2 and were caused by Defendant's breach of implied contract. These injuries are ongoing, imminent,  
3 immediate, and continuing.

4 251. As a direct and proximate result of Defendant's above-described breach of contract,  
5 Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

6 **COUNT III**  
7 **UNJUST ENRICHMENT**  
8 **(On Behalf of Plaintiff and the Class)**

8 252. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

9 253. This claim is pleaded solely in the alternative to Plaintiff's breach of implied  
10 contract claim.

11 254. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the  
12 form of valuable sensitive medical information that Defendant collected from Plaintiff and Class  
13 Members under the guise of keeping this information private. Defendant collected, used, and  
14 disclosed this information for their own gain, for marketing purposes, and for sale or trade with  
15 third parties.

16 255. Plaintiff and Class Members would not have used Defendant's services or would  
17 have paid less for those services, if they had known that Defendant would collect, use, and disclose  
18 their Private Information to third parties.

19 256. Defendant appreciated or had knowledge of the benefits conferred upon them by  
20 Plaintiff and Class Members.

21 257. As a result of Defendant's conduct, Plaintiff and Class Members suffered actual  
22 damages in an amount equal to the difference in value between their purchases made with  
23 reasonable data privacy practices and procedures that Plaintiff and Class Members paid for, and

1 those purchases without unreasonable data privacy practices and procedures that they received.

2 258. The benefits that Defendant derived from Plaintiff and Class Members rightly  
3 belong to Plaintiff and Class Members themselves. Under unjust enrichment principles, it would  
4 be inequitable for Defendant to retain the profit and/or other benefits it derived from the unfair and  
5 unconscionable methods, acts, and trade practices alleged in this Complaint.

6 259. Defendant should be compelled to disgorge into a common fund for the benefit of  
7 Plaintiff and Class Members all unlawful or inequitable proceeds it received as a result of its  
8 conduct and the unauthorized Disclosure alleged herein.

9 **COUNT IV**  
10 **BREACH OF FIDUCIARY DUTY**  
**(On Behalf of Plaintiff and the Class)**

11 260. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

12 261. A relationship existed between Plaintiff and the Class, on the one hand, and  
13 Defendant, on the other, in which Plaintiff and the Class put their trust in Defendant to protect the  
14 Private Information of Plaintiff and the Class, and Defendant accepted that trust.

15 262. Defendant breached the fiduciary duty that it owed to Plaintiff and the Class  
16 Members by failing to act with the utmost good faith, fairness, and honesty; failing to act with the  
17 highest and finest loyalty; and failing to protect and, indeed, intentionally disclosing, their Private  
18 Information.

19 263. Defendant's breach of fiduciary duty was a legal cause of injury-in-fact and  
20 damages to Plaintiff and the Class.

21 264. But for Defendant's breach of fiduciary duty, the injury-in-fact and damages to  
22 Plaintiff and the Class would not have occurred.

23 265. Defendant's breach of fiduciary duty substantially contributed to the injury and

1 damages to the Plaintiff and the Class.

2 266. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff  
3 and Class Members are entitled to and demand actual, consequential, and nominal damages,  
4 injunctive relief, and all other relief allowed by law.

5 **COUNT V**  
6 **INVASION OF PRIVACY—INTRUSION UPON SECLUSION**  
7 **(On Behalf of Plaintiff and the Class)**

8 267. Plaintiff re-allege and incorporate the above allegations as if fully set forth herein.

9 268. Plaintiff and Class Members had a reasonable expectation of privacy in their  
10 communications with Defendant via its Websites and Online Platforms.

11 269. Plaintiff and Class Members communicated sensitive PHI and PII—Private  
12 Information—that they intended for only Defendant to receive and that they understood Defendant  
13 would keep private.

14 270. Defendant's disclosure of the substance and nature of those communications to  
15 third parties without the knowledge and consent of Plaintiff and Class Members is an intentional  
16 intrusion on Plaintiff's and Class Members' solitude or seclusion in their private affairs and  
17 concerns.

18 271. Plaintiff and Class Members had a reasonable expectation of privacy given  
19 Defendant's representations in its Privacy Policies, and elsewhere. Moreover, Plaintiff and Class  
20 Members have a general expectation that their communications regarding healthcare with their  
21 healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is  
22 highly offensive to the reasonable person.

23 272. As a result of Defendant's tortious conduct, Plaintiff and Class Members have  
suffered harm and injury, including but not limited to an invasion of their privacy rights.

273. Plaintiff and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation, including monetary damages.

274. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to, damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

275. Plaintiff and Class Members are also entitled to punitive damages resulting from the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff and Class Members in conscious disregard of their rights. Such damages are needed to deter Defendant from engaging in such conduct in the future.

276. Plaintiff also seek such other relief as the Court may deem just and proper.

**COUNT VI**  
**INVASION OF PRIVACY**  
**CAL. CONST. ART. 1 § 1**  
**(On Behalf of Plaintiff and the Class)**

277. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

278. California established the right to privacy in Article I, Section I of the California Constitution.

279. Plaintiff and Class Members had a reasonable expectation of privacy in their communications with Defendant via its Websites and Online Platforms.

280. Plaintiff and Class Members communicated sensitive PHI and PII—Private Information—that they intended for only Defendant to receive and that they understood Defendant would keep private.

281. Defendant's disclosure of the substance and nature of those communications to third parties without the knowledge and consent of Plaintiff and Class Members is an intentional

1 intrusion on Plaintiff's and Class Members' solitude or seclusion in their private affairs and  
2 concerns.

3 282. Plaintiff and Class Members had a reasonable expectation of privacy given  
4 Defendant's representations in their Privacy Policies, and elsewhere. Moreover, Plaintiff and Class  
5 Members have a general expectation that their communications regarding healthcare with their  
6 healthcare providers will be kept confidential. Defendant's disclosure of PHI coupled with PII is  
7 highly offensive to the reasonable person.

8 283. As a result of Defendant's actions, Plaintiff and Class Members have suffered harm  
9 and injury, including but not limited to an invasion of their privacy rights under the California  
10 Constitution.

11 284. Plaintiff and Class Members have been damaged as a direct and proximate result  
12 of Defendant's invasion of their privacy and are entitled to just compensation, including monetary  
13 damages.

14 285. Plaintiff and Class Members seek appropriate relief for that injury, including but  
15 not limited to, damages that will reasonably compensate Plaintiff and Class Members for the harm  
16 to their privacy interests as a result of its intrusions upon Plaintiff's and Class Members' privacy.

17 286. Plaintiff and Class Members are also entitled to punitive damages resulting from  
18 the malicious, willful, and intentional nature of Defendant's actions, directed at injuring Plaintiff  
19 and Class Members in conscious disregard of their rights. Such damages are needed to deter  
20 Defendant from engaging in such conduct in the future.

21 287. Plaintiff also seek such other relief as the Court may deem just and proper.  
22  
23



**COUNT VII**  
**VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (“CIPA”),**  
**CAL. PENAL CODE §§ 630, *ET SEQ.***  
**(On Behalf of Plaintiff and the Class)**

288. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

289. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.* (“CIPA”) declaring that:

...advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.

The Legislature by this chapter intends to protect the right of privacy of the people of this state.

Cal. Penal Code §§ 630.

290. Cal. Penal Code § 631(a) prohibits persons from “aid[ing], agree[ing] with, employ[ing], or conspir[ing] with” a third party to “read[], or attempt[] to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained” “by means of any machine, instrument, or contrivance, or in any other manner...” Cal. Penal Code § 631(a).

291. Cal. Penal Code § 632(a) prohibits persons from intentionally recording confidential communications without consent of all parties to the communication.

292. All alleged communications between Plaintiff or Class Members and Defendant qualify as protected communications under CIPA because each communication is made using personal computing devices (e.g., computers, smartphones, tablets) that send and receive

1 communications in whole or in part through the use of facilities used for the transmission of  
2 communications aided by wire, cable, or other like connections.

3 293. As alleged in the preceding paragraphs, by use of the Meta Pixel and other tracking  
4 technologies, Defendant used a recording device to record the confidential communications  
5 without the consent of Plaintiff or Class members and then transmitted such information to others,  
6 such as Facebook.

7 294. At all relevant times, Defendant's aiding of Facebook, and other third parties to  
8 learn the contents of communications and Defendant's recording of confidential communications  
9 was without Plaintiff's and the Class Members' authorization and consent.

10 295. Plaintiff and Class Members had a reasonable expectation of privacy regarding the  
11 confidentiality of their communications with Defendant. Defendant promised them that it would  
12 safeguard their personal information, and that "[o]ther uses and disclosures not described in this  
13 notice will be made only with your written authorization, such as sale of medical information..."<sup>113</sup>  
14 Defendant never received any authorization and disclosed Plaintiff's and the Class's Private  
15 Information anyways.

16 296. Defendant engaged in and continued to engage in interception by aiding others  
17 (including Facebook) to secretly record the contents of Plaintiff's and Class Members' wire  
18 communications.

19 297. The intercepting devices used in this case include, but are not limited to:

- 20 a. those to which Plaintiff's and Class Members' communications were  
21 disclosed;  
22 b. Plaintiff's and Class Members' personal computing devices;  
23

---

<sup>113</sup> *Notice of Privacy Practices*, **Exhibit B**.

- c. Plaintiff's and Class Members' web browsers;
- d. Plaintiff's and Class Members' browser-managed files;
- e. the Meta Pixel;
- f. internet cookies;
- g. other pixels, trackers, and/or tracking technology installed on Defendant's Website and/or server;
- h. Defendant's computer servers;
- i. third-party source code utilized by Defendant; and
- j. computer servers of third parties (including Facebook).

298. Defendant aided in the interception of contents in that the data from the communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the third parties, including Facebook, include information which identifies the parties to each communication, their existence, and their contents.

299. Plaintiff and Class Members reasonably expected that their Private Information was not being intercepted, recorded, and disclosed to Facebook, and other third parties.

300. No legitimate purpose was served by Defendant's willful and intentional disclosure of Plaintiff's and Class Members' Private Information to Facebook, and other third parties. Neither Plaintiff nor Class Members consented to the disclosure of their Private Information by Defendant to Facebook, and other third parties.

301. The tracking pixels that Defendant utilized are designed such that they transmitted each of a website user's actions to third parties alongside and contemporaneously with the user initiating the communication. Thus, Plaintiff and Class Members' communications were intercepted in transit to the intended recipient (Defendant) before they reached Defendant's

1 servers.

2 302. Defendant willingly facilitated Facebook's interception and collection of Plaintiff's  
3 and Class Members' Private Information by embedding pixels on its Online Platforms. Moreover,  
4 Defendant had full control over these tracking pixels, including which webpages contained the  
5 pixels, what information was tracked and shared, and how events were categorized prior to  
6 transmission.

7 303. Defendant gave substantial assistance to Facebook in violating the privacy rights  
8 of its patients, despite the fact that Defendant's conduct constituted a breach of the duties of  
9 confidentiality that medical providers owe their patients. Defendant knew that the installation of  
10 the Meta Pixel on its website would result in the unauthorized disclosure of its patients'  
11 communications to Facebook, yet nevertheless did so anyway.

12 304. Plaintiff's and Class Members' electronic communications were intercepted during  
13 transmission, without their consent, for the unlawful and/or wrongful purpose of monetizing their  
14 Private Information, including using their sensitive medical information to develop marketing and  
15 advertising strategies. The private information that Defendant assisted Facebook, and other third  
16 parties with reading, learning, and exploiting, including Plaintiff's and Class Member's medical  
17 conditions, their medical concerns, and their past, present, and future medical treatment.

18 305. Plaintiff and the Class Members seek statutory damages under Cal. Penal Code §  
19 637.2(a), which provides for the greater of: (1) \$5,000 per violation; or (2) three times the amount  
20 of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as  
21 injunctive or other equitable relief.

22 306. In addition to statutory damages, Defendant's violations caused Plaintiff and Class  
23 Members the following damages.